Základy kybernetická bezpečnost

PRŮVODCE

Co-funded by the Erasmus+ Programme of the European Union

Příručka je jedním z výsledků projektu Erasmus+ "Základy kybernetické bezpečnosti".

Koordinátor projektu:
Lipinski University (WSEPiNM) Kielce, Polsko

Partneři:
Ambis vysoká škola, Praha, Česká republika
Instituto Politécnico de Beja, Portugalsko

Co-funded by the Erasmus+ Programme of the European Union

Co je to za publikaci?

Jedná se o příručku pro vyučujícího kurzu/semestru, která slouží k využití sbírky online materiálů nalezených na platformě Základy kybernetické bezpečnosti. Příručka bude užitečná také pro studenty, zejména pro ty, kteří studují samostatně.

Materiály byly vytvořeny v rámci projektu "Základy kybernetické bezpečnosti", financovaného z fondů EU v rámci programu Erasmus+ v letech 2019 až 2022. Projekt koordinovala WSEPiNM v Kielcích a partnery byly univerzity z České republiky a Portugalska.

Online materiály (videopřednášky, učebnice k jednotlivým tématům, instruktážní videa) jsou určeny k lepšímu pochopení širokého kontextu kybernetické bezpečnosti a k rozvoji dovedností, jak se vypořádat s různými typy hrozeb. Celek lze přizpůsobit různým vzdělávacím kontextům v závislosti na potřebách.

Publikace obsahuje podrobné materiály a pokyny pro vedení *kombinované výuky* nebo *online* seminářů.

Výběr a pořadí prezentovaných témat by měl být přizpůsoben potřebám konkrétní skupiny účastníků, a proto záleží na konkrétním vedoucím třídy nebo kurzu. Neexistuje požadavek na provedení všech modulů nebo na jejich přesné pořadí navržené v tomto zdroji.

Pro koho je tato publikace určena?

Tato publikace je určena akademickým pracovníkům a školitelům v oblasti bezpečnosti počítačových systémů. Navrhuje se flexibilní přístup: kurz lze začlenit do stávajících učebních osnov nebo jej nabízet jako samostatný vzdělávací kurz. Přestože je materiál určen pro vysokoškolský sektor, bude užitečný i pro ty, kteří školí pracující. Z geografického hlediska je bezprostředním kontextem materiálu publikum v partnerských zemích, ale vzhledem k nadnárodnímu přístupu a povaze předkládaných témat je materiál snadno přizpůsobitelný potřebám pedagogů v jiných zemích.

Jaké jsou cíle této publikace?

Hlavními příjemci projektu "Základy kybernetické bezpečnosti" jsou studenti různých fakult, protože v dnešní době je těžké najít oblast života, ve které by hrozba útoků na IT systémy nebyla problémem. Kurz lze doporučit zejména studentům oborů, jako je vnitřní bezpečnost, neboť kybernetické útoky na různé instituce jsou dnes nesrovnatelně častější (a výnosnější) než fyzické útoky. Cílem této publikace je pomoci vedoucímu kurzu/třídy vybrat si z mnoha navržených online materiálů ty, které jsou pro jeho skupinu studentů užitečné, a vést výuku smíšenou (aktivity ve třídě a samostatná online práce studenta) nebo zcela online. V případě kombinované výuky je vhodné použít metodu převrácené třídy, kdy studenti přicházejí do třídy po přečtení předem připravených online materiálů.

Pedagogický přístup

"Znalosti vytvářejí studenti".

Kurz využívá Kolbův (1984) přístup k zážitkovému učení. Podle Kolbova cyklu se v procesu učení opakuje cyklus čtyř kroků: zkušenost, reflexe, zobecnění a aplikace.

Odborná příprava odborníků na kybernetickou bezpečnost se ve velké míře opírá o zkušenostní učení - o stále obtížnější úkoly a zároveň o rozvoj znalostí a dovedností.

Ve všech aktivitách navržených pro použití ve třídě se snažíme ukázat vztah probíraného tématu ke každodenní pracovní praxi účastníků kurzu, abychom jim v souladu se zásadami Human Centered Design poskytli poutavý vzdělávací zážitek.

Poznámky pro školitele

Poznámky pro instruktory vycházejí z obsahu online modulů a řídí se pořadím modulů na platformě. Předpokládá se, že každé sezení bude trvat přibližně dvě vyučovací hodiny. Popis hodinového zatížení je uveden v sylabu každého modulu. Sezení lze také prodloužit nebo zkrátit vhodnými změnami materiálů a témat.

Vybavení a materiály

Vybavení a materiály potřebné pro jednotlivé semináře jsou běžně dostupné v sektoru vysokoškolského vzdělávání. Patří k nim počítačová učebna vhodná pro interaktivní skupinovou práci, projektor, plátno, přístup k internetu, reproduktory, flipchart, pera atd.

Využití kurzu

Přejít na: https://moodle.cybersecurity-fundamentals.eu/

Vyberte jazyk a modul kurzu.

Zvolte status (je možné se přihlásit jako "Host", ale tím se omezí přístup k některým materiálům a funkcím). Účet je možné si vytvořit sám a přihlásit se pomocí účtu Google nebo Microsoft.

Materiály kurzu lze používat postupně nebo výběrově podle potřeby.

Informace pro univerzity

Každá univerzita může tento kurz snadno hostovat na svém serveru a používat jej ke vzdělávání svých studentů. LMS tohoto kurzu je Moodle, populární bezplatná e-learningová platforma s otevřeným zdrojovým kódem. Kurz je rovněž zdarma.

Zájemci z řad vysokých škol nás mohou kontaktovat na adrese: erasmus@wsepinm.edu.pl . Zájemci obdrží balíček kurzu, který mohou během několika minut spustit na vlastním serveru. To platí nejen pro polskou, ale také pro anglickou, českou a portugalskou jazykovou verzi. Zvláště bychom chtěli upozornit na možnost využití anglické verze kurzu pro výuku v tomto jazyce, který se v kyberprostoru orientuje obtížně, už jen kvůli převaze anglické terminologie.

Obsah kurzu

Obsah výuky je rozdělen do následujících modulů:

Úvod

Modul 1: Základy počítačových sítí

Modul 2: Zákony a další předpisy

Modul 3: Odhalování a prevence kybernetických hrozeb

Modul 4: CSIRT a CERT

Modul 5: Základy počítačové forenziky

Modul 6: Komplexní zabezpečení sítě

Modul 1

Základy počítačových sítí

1. Úvod

1.1 Shrnutí modulu

Modul se zaměřuje na základní pojmy počítačových sítí (např. protokoly, adresy, topologie atd.) a je určen pro ty, kteří se s problematikou počítačových sítí dosud nesetkali. Studenti informatiky budou pravděpodobně moci tento modul vynechat.

1.2 Cíle kurzu

Cílem modulu je seznámit se základními koncepty základů sítí. Je určen těm, kteří se dosud nesetkali s tématy konfigurace sítě, protokolů, topologie sítě atd.

Po absolvování kurzu kombinovanou formou výuky by měl student získat schopnost nastavit jednoduchou místní síť, připojit ji k internetu, otestovat výkon sítě a odstranit závady.

Takto získané znalosti jsou nezbytné k pochopení toho, co je to internet a jaká nebezpečí hrozí při pouhém připojení k síti.

1.3 Obsah kurzu

Jednotlivé přednášky seznamují studenty s fyzickou a logickou vrstvou sítě. Studenti se seznámí s pojmy protokoly, datové pakety, fyzické a logické adresy a základní síťové služby.

1.4 Cíle učení

- Získat základní znalosti o počítačových sítích, síťové infrastruktuře.
- Seznámení se síťovou architekturou LAN, MAN, WAN.
- Seznámení se sedmivrstvým modelem ISO/OSI
- Seznámení se s hodnotovým modelem sítě TCP/IP. Znalost základů protokolů TCP a UDP.
- Znalost základů komunikace VoIP.
- Porozumění problematice výkonnosti sítě. Seznámení se s metodami snižování síťového provozu.
- Používání počítačů, digitálních nástrojů a počítačových sítí, včetně znalosti principů digitálních zařízení a počítačových sítí a provádění základních testů počítačových sítí.

1.5 Sylabus

Efekt učení	Studenti, kteří absolvovali předmět ví/umí/může:
NOVINKY	
W1	Charakterizuje služby sítě/serveru
W2	Má rozsáhlé a strukturované znalosti služeb a aplikací používaných v počítačových sítích. zná síťové operační systémy
W3	má znalosti o konfiguraci síťových zařízení
W4	má znalosti o rizicích v počítačových sítích. Rozumí významu a úloze vybraných síťových protokolů s přiřazením ke konkrétním vrstvám referenčního modelu.
W5	má znalosti o návrhu počítačové sítě a jejích součástí
W6	Popisuje a analyzuje třídy IP adres
W7	Umí pojmenovat vrstvy ISO/OSI
W8	Rozpozná topologie místních sítí
W9	Zná adresy portů TCP/UDP
W10	Zná pojmy týkající se: správy a řízení počítačových sítí
W11	Zná principy síťových zařízení
DOVEDNOSTI	
U1	Popisuje a analyzuje třídy IP adres
U2	Připojení místní počítačové sítě k internetu
U3	Umět analyzovat provoz v počítačových sítích. Umět konfigurovat síťové adresování a vybrané bezpečnostní prvky.
U4	Umět konfigurovat základní síťová zařízení. Zná a umí používat simulační nástroje při analýze a návrhu počítačových sítí.
U5	Schopnost konfigurovat servery webových služeb
U6	Umět nakonfigurovat pracovní stanici pro práci v síti.
U7	Může zkontrolovat výkon sítě
U8	Umět navrhnout místní síť
U9	Umět vytvořit jednoduchou místní síť s použitím skutečného síťového vybavení. Umí samostatně připravit strukturovanou kabeláž.
U10	schopnost vzdáleně spravovat pracovní stanice v síti
U11	Navrhuje strukturu adres IP v síti
U12	Rozpoznává a používá normy pro strukturovanou kabeláž.
U13	Rozpozná protokoly místní sítě a přístupové protokoly rozsáhlé sítě.
U14	Rozpozná síťová zařízení (popis, symbol, vzhled).
U15	Provádí měření a testy logické sítě.
SOCIÁLNÍ KOMPETENCE	
K1	Popisuje konfiguraci síťových rozhraní.
K2	být schopen určit priority pro opatření
K3	Schopnost pracovat a komunikovat ve skupině, pokud jde o konfiguraci adresování a vybraných síťových služeb.
K4	Schopnost pracovat v týmu, řešit úkoly společně
K5	vysvětluje principy protokolů počítačových sítí.

Obsah modulu (program přednášek a dalších aktivit)		Odkaz na výsledky učení
PŘEDNÁŠKY 1. Fyzická struktura sítě, typy síťových zařízení, kabely 2. Datové jednotky v sítích 3. Logická struktura sítě, topologie 4. Modely ISO/OSI, TCP/IP 5. Diskuse o používání vrstev WORKSHOPY 1. Vytvoření fyzické sítě 2. Konfigurace sítě 3. Průzkum sítě 4. Síťové připojení k internetu		W 1-11 U1-15 K1-5
Zůstatek kreditů ECTS		
Forma pracovní zátěže studentů		Počet hodin
Počet hodin s přímou účastí akademického pracovníka		
1.1	Účast na přednáškách	6
1.2	Účast na seminářích	
1.3	Účast na seminářích	30
1.4	Účast na laboratorních činnostech	
1.5	Účast na projektech	
1.6	Účast na konzultacích (2-3krát za semestr)	
1.7	Účast na konzultacích k projektu	
1.8	Účast na zkouškách/testech	2
1.9	Ostatní ...	
1.10	**Počet hodin strávených za přímé asistence akademických pracovníků (součet 1.1 - 1.9)**	38
1.11	**Počet ECTS kreditů, které student získal v předmětech vyžadujících přímou účast akademického pracovníka)**	1,5
Individuální práce studentů		
2.1	Individuální studium (včetně e-learningových přednášek)	10
2.2	Individuální příprava na semináře	10
2.3	Individuální příprava na test	
2.4	Individuální příprava na laboratorní výuku	
2.5	Příprava zpráv	
2.6	Realizace samostatně prováděných úkolů (projekty, dokumentace)	
2.7	Příprava na závěrečnou zkoušku/testy semináře	10
2.8	Příprava na závěrečnou zkoušku/testování přednášek	
2.9	Další	
2.10	**Počet hodin individuální práce (součet 2.1 - 2.9)**	30
2.11	**Počet ECTS kreditů, které student získal za jednotlivé výukové úkoly**	1
Celková pracovní zátěž (h)		**68**
ECTS kredity za modul		**2,5**

Metody ověřování výsledků učení									
Výsledek učení	Formy hodnocení								
	Ústní zkouška	Písemná zkouška	Částečný písemný úkol	Závěrečný písemný úkol (esej atd.)	Test	Design/prezentace	Nahlásit	Činnosti ve třídě	Ostatní ...
NOVINKY									
W1-11					x			x	
DOVEDNOSTI									
U1-15					x			x	
SOUTĚŽE									
K1-5								x	

Kritéria pro hodnocení kompetencí studentů
Níže jsou shrnuty minimální požadavky na tři skupiny výsledků učení, které musí student splnit, aby předmět absolvoval. Aby student modul absolvoval, musí být všechny výsledky učení popsané v sylabu kladně ověřeny osobou (osobami), která (které) modul vyučuje (vyučují).

W - VĚDOMOSTI
Hodnocení:
Uspokojivý - Student si pamatuje a reprodukuje znalosti, které má v rámci modulu zvládnout.
Dobrý - Žák dodatečně interpretuje jevy / problémy a je schopen vyřešit typický problém.
Velmi dobře -Student je schopen řešit i složité problémy v dané oblasti, je schopen syntetizovat, provést komplexní hodnocení, vytvořit práci, která je originální a inspirativní pro ostatní.

U - DOVEDNOSTI
Hodnocení:
uspokojivý - student zná podstatu činností a je schopen pod vedením akademického učitele provádět činnosti/řešit problémy související s obsahem modulu.
Dobrý - Student je schopen samostatně provádět činnosti / úkoly / řešit typické problémy související s obsahem modulu.
Velmi dobře - Student si plně osvojil schopnost / dovednost provádět činnosti / úkoly / problémy stanovené v obsahu modulu, a to i ve složitějších případech.

K - SOCIÁLNÍ KOMPETENCE
Hodnocení:
uspokojivě - student pasivně vstřebává obsah modulu, prokazuje schopnost soustředit se a naslouchat.
Dobrý - Žák se aktivně účastní výuky, vytváří hodnotové soudy podle kritérií přijatých v daném oboru, dokáže aktivně spolupracovat ve skupině.
Velmi dobře - Žák integruje postoje podle navrženého modelu, rozvíjí vlastní systém profesních a společenských hodnot, je schopen převzít odpovědnost za jednání skupiny, včetně vedení.

2. Základní materiály pro učitele

Definice (slovníček pojmů)

Počítačová síť - soubor zařízení, jako jsou počítače, tiskárny, telefony a televizory, která jsou vzájemně propojena za účelem výměny dat. K propojení zařízení se používá přenosové médium a k přenosu dat se používá komunikační protokol.

Adresa IPv4 - Jedná se o 32bitové číslo, které se pro snadnější použití zadává v desítkové soustavě (např. 192.168.31.190) a slouží k identifikaci zařízení a adresování dat v síti.

HOST - Jedná se o zařízení s adresou IP, které je zdrojem nebo příjemcem dat přenášených po síti, tj. přijímá data od jiných zařízení nebo tato data odesílá. Termín hostitel se někdy používá zaměnitelně s termínem koncové zařízení, protože obvykle označuje počítač, tablet nebo chytrý telefon, tj. zařízení, se kterým je uživatel sítě v přímém kontaktu.

Klient - Zařízení, přesněji jeho software, využívá služby poskytované serverem. Nejběžnějším klientem je dnes webový prohlížeč, který umožňuje prohlížet obsah webových stránek umístěných na webovém serveru. Příkladem klienta může být také FileZilla, která umožňuje výměnu souborů přes internet, a nejrůznější e-mailový software usnadňující používání pošty. Klienty budou také herní konzole nebo chytré telefony, samozřejmě pokud jsou připojeny k internetu.

Server - počítač s nainstalovaným specializovaným softwarem, který slouží ostatním počítačům. Služba, kterou může server poskytovat, je například webová stránka, e-mail nebo zdroj souborů. Serverem může být jakýkoli počítač, na kterém je takový software nainstalován a nakonfigurován, například APACHE, který se používá k údržbě a sdílení webových stránek, nebo MySQL, což je systém pro správu databází. Server je obvykle vyhrazený počítač s vysokým výpočetním výkonem, který je schopen zpracovávat mnoho připojení a dotazů současně.

Přenosové médium - Jinými slovy médium, které je síťovým prvkem, jehož prostřednictvím spolu zařízení komunikují a vyměňují si data. Tímto médiem může být měděný kabel, optický kabel a rádiové vlny (WiFi).

Komunikační protokol - Jedná se o způsob nebo jazyk komunikace a výměny dat mezi zařízeními, který definuje pravidla a zásady této komunikace.

Internet - Jedná se o soubor vzájemně propojených rozsáhlých sítí, které tvoří globální počítačovou síť. Počátky internetu sahají až k vytvoření sítě ARPANET na konci 60. let 20. století a první internetové připojení v Polsku bylo spuštěno v září 1990. Mnozí vnímají internet jako soubor stránek k prohlížení, ale není tomu tak, protože internet je souborem mnoha rozsáhlých sítí rozmístěných po celém světě a webové stránky jsou specifické síťové služby.

Intranet - jedná se o soukromou interní síť, která používá stejné komunikační standardy (protokoly) jako internet, ale přístup k ní mají pouze oprávnění uživatelé, například zaměstnanci dané společnosti. Ve většině případů je přístup do intranetu, resp. do této vnitřní podnikové sítě, prostřednictvím webové stránky, takže se říká, že komunikace využívá stejné standardy jako internet.

Extranet - je rozsáhlá odrůda intranetu, která umožňuje přístup ke svým zdrojům nejen zaměstnancům dané společnosti, ale i dalším uživatelům.

DNS (Domain Name System) - síťová služba, jejímž úkolem je změnit lidsky čitelné jméno, tzv. mnemotechnické jméno, na IP adresu zařízení v síti. Jedná se o základní službu

internetu, která mění adresy webových stránek na odpovídající IP adresy serverů, kde jsou tyto stránky uloženy, např. změna internetové adresy onet.pl na IP adresu 214.180.141.140.

Protokol **DHCP** (Dynamic Host Configuration Protocol) je automatický konfigurační protokol, který hostiteli přiřazuje IP adresu, masku podsítě nebo adresu výchozí brány. Jedná se o nejběžnější metodu přidělování IP adres počítačům v síti, protože nevyžaduje ruční konfiguraci IP adresy v každém počítači.

3. Během výuky

Několik nápadů na aktivity:

WORKSHOPY

Spolu se studenty vytvořte ve studiu místní síť a připojte ji k internetu.

Společně se studenty nainstalujte zástrčku RJ45 na kabel UTP a zkontrolujte výkon kabelu.

KONTROLNÍ OTÁZKY

- Které protokoly se používají pro e-mail a které pro webové stránky?

- Vyjmenujte 7 vrstev modelu ISO/OSI?

- Co je to adresa MAC a co je to adresa IP?

- Co znamenají pojmy zapouzdření a dekapsulace?

- Jak se IPv4 liší od IPv6?

- Jaké jsou hlavní výhody a nevýhody optických vláken ve srovnání s kroucenou dvojlinkou?

PRÁCE VE DVOJICÍCH/SKUPINÁCH

Scénář "hluchého telefonu" v různých konfiguracích sítě:

1. Rozdělte se do skupin: Rozdělte účastníky do skupin, každá skupina by se měla skládat nejméně ze tří osob.

2. Lineární konfigurace: V první konfiguraci by měla být síť nastavena lineárně. První osoba ve skupině vymyslí krátkou větu a poté ji předá další osobě prostřednictvím "hloupého telefonu". Poslední osoba ve skupině předá větu nahlas. Porovnejte přijatou větu s původní a diskutujte s účastníky o tom, jak se sdělení změnilo.

3. Hvězdicová konfigurace: V druhé konfiguraci by měla být síť nastavena hvězdicově. Vyberte jednu osobu, která bude začínat předávání věty. Tato osoba předá větu další osobě, která ji předá další osobě a tak dále, dokud větu neslyší všichni lidé ve skupině. Porovnejte přijatou větu s původní větou a diskutujte s účastníky o tom, jak se sdělení změnilo.

4 Konfigurace mřížky: Ve třetí konfiguraci by měla být mřížka rozestavěna mřížkovým způsobem. Každá osoba ve skupině by měla mít dva sousedy a jednomu z nich předat větu. Podívejte se, jak se věta mění, když prochází přes různé osoby, a diskutujte o tom s účastníky.

Po každé konfiguraci mřížky prodiskutujte s účastníky, jaké poznatky lze z tohoto cvičení vyvodit v souvislosti s topologií počítačové sítě. Příklady otázek, které můžete položit, jsou následující:

- Jak různé konfigurace sítě ovlivňují kvalitu přenosu informací?
- Jaké problémy mohou nastat při různých konfiguracích sítě?
- Jaké jsou výhody a nevýhody různých topologií sítě v kontextu přenosu informací?

TÉMATA K DISKUSI

- Kdo vlastní internet, kdo ho ovládá?
- Jaká jsou rizika otevřeného přístupu na web?
- Měla by být zavedena větší kontrola obsahu na internetu? Kdo by ji měl provádět?
- Jaké další sítě kromě počítačových lze rozpoznat? Jak se mění přístup k ochraně soukromí v závislosti na velikosti sítě a dalších faktorech?
- Může být restaurace příkladem řetězce? Jaké jsou role zákazníků, číšníků a kuchařů? Jak vypadají protokoly a datové pakety?

4. Internetové zdroje

https://learn.microsoft.com/pl-pl/training/modules/network-fundamentals/
https://www.icann.org/
https://isportal.pl/
https://www.speedtest.net/
https://www.intgovforum.org/
https://www.whatismyisp.com/
https://uke.gov.pl/

5. Další otázky/testy

Co znamená zkratka VoIP?
A. Hlas na internetovém protokolu
B. Vice over Internet Protocol
C. Hlas přes internet
D. Hlas přes internetový protokol
ODPOVĚĎ: D

Prvním "technickým" kyberzločincem byl Leonard Kleinrock, který v roce 1973 odeslal prostřednictvím sítě ARPANET zprávu týkající se:
A. jeho ztracený elektrický holicí strojek.
B. jeho přítelkyně
C. požadovaná učebnice
D. písně
ODPOVĚĎ: A

Jak se jmenuje program, který funguje jako telefonní ústředna?
A. IP-PBX
B. CVoIP
C. Skype
D. MS Teams
ODPOVĚĎ: A

Který z následujících programů nepoužívá technologii VoIP?
A. MS Teams
B. Zoom
C. Google Meet
D. Photoshop
ODPOVĚĎ: D

Co je program Asterix?
A. Server SIP
B. souborový server
C. fotoserver
D. kompresor souborů
ODPOVĚĎ: A

Která z následujících možností nemá vliv na výkon počítačové sítě?
A. Pasivní části počítačové sítě
B. aktivní zařízení
C. elektromagnetické rušení
D. atmosférický tlak
ODPOVĚĎ: D

Z jakého materiálu je vyrobena kroucená dvojlinka?
A. měď
B. hliník
C. ocel
D. sklolaminát
ODPOVĚĎ: A

Síťový kabel s kroucenou dvojlinkou kategorie 5 umožňuje přenos až do maximální rychlosti:
A. 1 Gb/s
B. 100 Mb/s
C. 1 Mb/s
D. 10 Gb/s
ODPOVĚĎ: A

Které médium přenáší data na větší vzdálenost?
A. optické vlákno
B. měděný kabel (kroucená dvojlinka)
C. ocelové lano
D. hliníkový kabel
ODPOVĚĎ: A
Co je to HOST v počítačové síti?
A. jakékoli zařízení připojené k síti
B. hostitel
C. centrální zařízení v počítačové síti
D. externí disk
ODPOVĚĎ: A

Co je to síťová karta?
A. zařízení, které umožňuje hostiteli připojit se k počítačové síti.
B. součást hlavního procesoru
C. napájecí zařízení
D. SSD
ODPOVĚĎ: A

Který program lze použít k měření rychlosti stahování v počítačové síti?
A. wget
B. ping
C. MS Teams
D.
ODPOVĚĎ: A

Webová adresa, na které můžete zkontrolovat výkon sítě, je:
A. speedtest.net
B. google.com
C. yahoo.com
D. google.net
ODPOVĚĎ: A

Domácí síťový směrovač lze použít k:
A. omezení síťového provozu
B. vyhledávání informací
C. video dohled
D. přehrávání mp3
ODPOVĚĎ: A

Zadáním "CMD" v MS Windows 10/11 do vyhledávacího okna spustíme:
A. příkazový řádek
B. konfigurace síťové karty
C. kalkulačka
D. program pro kompresi souborů
ODPOVĚĎ: A

K čemu slouží program ping?
A. označuje dobu odezvy na odeslaný paket
B. mění čas systému
C. zobrazí příručku nápovědy
D. ukončit všechny programy
ODPOVĚĎ: A

Který program vrátí seznam po sobě jdoucích směrovačů na trase k cílovému počítači v síti?
A. Tracert
B. wget
C. ping
D. span
ODPOVĚĎ: A

Modul 2

Zákony a předpisy

3. Úvod

1.5 Shrnutí kurzu

Kurz se zaměřuje na základní právní pojmy související s internetem a seznamuje studenty s tématem odpovědnosti v kyberprostoru. Pro pochopení celé problematiky je rovněž nezbytná znalost právních základů poskytovatele internetových služeb (ISP). Významná část kurzu se zabývá kybernetickou bezpečností a odpovídajícími právními předpisy. Kromě toho nelze opomenout ochranu osobních údajů v kyberprostoru. Ochrana soukromí a bezpečnost v oblasti informačních a komunikačních technologií a ochrana údajů v kyberprostoru jsou rovněž klíčovými tématy, která tvoří podstatnou část kurzu.

1.2 Cíle kurzu

Studenti se seznámí se vztahem mezi právem a kyberprostorem. Seznámí se s právním základem poskytovatelů internetových služeb (ISP). Při studiu se navíc zaměří na kybernetickou bezpečnost a její regulaci. Kromě toho budou studenti studovat systém řízení informační bezpečnosti. V neposlední řadě zjistí, jaký význam má ochrana dat v kyberprostoru.

Cílem modulu je seznámit studenty s aplikací práva v oblasti informačních a komunikačních technologií. Dalším cílem je identifikovat právní hranice kybernetické bezpečnosti.

Po absolvování kurzu by měl student získat schopnost orientovat se v právních normách Evropské unie a zúčastněných zemí, které přímo souvisejí s problematikou kybernetické bezpečnosti.
Kromě toho student získá základní přehled o problematice občanského a veřejného práva, které se uplatňuje v kyberprostoru, se zvláštním zaměřením na praktické využití získaných znalostí v praxi. Student se seznámí nejen s teorií aplikace práva v kyberprostoru a úpravou de lege lata, ale také s praktickou aplikací práva v praxi (de lege aplicata).

Získané znalosti budou dále využity v modulech o kybernetických útocích a obraně proti nim a v modulu o budování a fungování bezpečnostních týmů.

1.3 Obsah kurzu

Jednotlivé přednášky seznamují studenty s daným právním systémem, právní normou, právem a internetem. Dále se studenti seznámí s odpovědností v kyberprostoru a s právním základem poskytovatelů internetových služeb (ISP). Jedním z klíčových témat je kybernetická bezpečnost a její právní úprava. Mimořádně důležitá je také ochrana soukromí a s ní související bezpečnost v ICT, ochrana dat v kyberprostoru, proto je jim věnována poslední část přednášek.

1.4 Cíle učení

1) Úvod do problematiky právního systému, právní normy, práva a internetu
2) Odpovědnost v kyberprostoru
3) Porozumět právnímu základu podnikání poskytovatele internetových služeb (ISP).
4) Ochrana osobních údajů v kyberprostoru
5) Ochrana soukromí a bezpečnost v IKT, ochrana údajů v kyberprostoru

3.5 Potřebné vybavení a materiály

Zákony a předpisy o kybernetické bezpečnosti - k dispozici online

Primární právo EU

- Listina základních práv Evropské unie

Směrnice Evropského parlamentu a Rady

- 91/250/EHS o právní ochraně počítačových programů
- 98/34/ES o postupu při poskytování informací v oblasti technických norem a předpisů, ve znění směrnice 98/48/ES.
- 1999/5/ES o rádiových zařízeních a telekomunikačních koncových zařízeních a vzájemném uznávání jejich shody
- 2000/31/ES o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu (směrnice o elektronickém obchodu).
- 2002/19/ES o přístupu k sítím elektronických komunikací a přiřazeným zařízením a o jejich vzájemném propojení (přístupová směrnice).
- 2002/20/ES o oprávnění pro sítě a služby elektronických komunikací (autorizační směrnice), ve znění směrnice 2009/140/ES.
- 2002/21/ES o společném předpisovém rámci pro sítě a služby elektronických komunikací (rámcová směrnice), ve znění směrnice 2009/140/ES.
- 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací (směrnice o univerzální službě).
- 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací.
- 2006/24/ES o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí.
- 2008/114/ES o určování a označování evropské kritické infrastruktury a o posouzení potřeby zvýšit její ochranu.
- 2011/93/EU o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii, kterým se nahrazuje rámcové rozhodnutí Rady 2004/68/SVV.
- 2013/11/EU o alternativním řešení spotřebitelských sporů a o změně nařízení (ES) č. 2006/2004 a směrnice 2009/22/ES (směrnice o alternativním řešení spotřebitelských sporů)
- 2013/40/EU o útocích na informační systémy, kterým se nahrazuje rámcové rozhodnutí Rady 2005/222/SVV
- 2015/1535 o postupu při poskytování informací v oblasti technických předpisů a pravidel pro služby informační společnosti
- (EU) 2015/2366 o platebních službách na vnitřním trhu, kterou se mění směrnice 2002/65/ES, 2009/110/ES a 2013/36/EU a nařízení (EU) č. 1093/2010 a zrušuje směrnice 2007/64/ES ("revidovaná směrnice o platebních službách").
- 2016/680 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV
- 2016/1148 o opatřeních pro vysokou společnou úroveň bezpečnosti sítí a informačních systémů v Evropské unii (NIS)

Nařízení Evropského parlamentu a Rady

- 460/2004/ES o zřízení Evropské agentury pro bezpečnost sítí a informací, ve znění nařízení č. 1007/2008.

- 1077/2011/ES o zřízení Evropské agentury pro provozní řízení rozsáhlých informačních systémů v prostoru svobody, bezpečnosti a práva
- 526/2013 o Agentuře Evropské unie pro bezpečnost sítí a informací (**ENISA)** a o zrušení nařízení (ES) č. 460/2004 Text s významem pro EHP
- 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (**eIDAS)**[1]
- 679/2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů - **GDPR)**.

Rozhodnutí Rady Evropy

- 92/242/EHS v oblasti bezpečnosti informačních systémů
- **2005/222/SVV o útocích na informační systémy**
- 2011/292/EU o bezpečnostních pravidlech pro ochranu utajovaných informací EU

Další dokumenty

- Úmluva Rady Evropy č. 185 o kyberkriminalitě
- Dodatkový protokol 189 k Úmluvě o kyberkriminalitě Rady Evropy
- Úmluva Rady Evropy č. 196 o předcházení terorismu
- Prováděcí nařízení Komise (EU) 2018/151, kterým se stanoví prováděcí pravidla ke směrnici Evropského parlamentu a Rady (EU) 2016/1148, pokud jde o další vyjasnění prvků, které by poskytovatelé digitálních služeb měli zohlednit při řízení rizik pro bezpečnost sítí a informačních systémů, a parametrů pro určení, zda má incident významný dopad.

Mezinárodní normy

- Řada ISMS ISO/IEC 27000

Další

- Návrh NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY o jednotném digitálním trhu služeb (Akt o digitálních službách) a o změně směrnice 2000/31/ES
- Soukromoprávní a veřejnoprávní odpovědnost za jednání uživatele nebo společnosti v online prostředí
- Charakteristika a definice různých poskytovatelů internetových služeb a jejich práv a povinností v oblasti kybernetické bezpečnosti
- ISMS a vztah k zákonu o kybernetické bezpečnosti

[1] Dále jen "**eIDAS".**

1.6 Sylabus

Výsledek učení	Student, který úspěšně absolvuje tento modul, bude znát/umět následující.
NOVINKY	
W1	Student získá odborné znalosti a rozšíří si právní povědomí o informačních a komunikačních technologiích.
W2	Student získá odborné znalosti týkající se právní definice kybernetické bezpečnosti podle mezinárodního práva (zejména práva EU) a vnitrostátního práva zúčastněných zemí.
DOVEDNOSTI	
U1	Je schopen identifikovat jednotlivé poskytovatele internetových služeb, jejich práva a povinnosti a na základě této identifikace je schopen argumentovat v oblastech práva souvisejících s kybernetickou bezpečností.
U2	Umět analyzovat základní rámec aktiv v kyberprostoru (např. technologie, procesy, data atd.) a určit právní doporučení pro jejich ochranu.
SOUTĚŽE	
K1	Student částečně ovládá právní předpisy, je schopen aplikovat jednotlivé právní instituty na případové studie.

Obsah modulu (program přednášek a dalších aktivit)	**Odkaz na výsledky učení**
PŘEDNÁŠKY 1. Mezinárodní právní normy upravující kyberkriminalitu 2. Vnitrostátní právní normy upravující kyberkriminalitu WORKSHOPY 1. Analýza jednotlivých kybernetických útoků a jejich subsumpce pod ustanovení Úmluvy o kyberkriminalitě (ESD č. 185) a vnitrostátní právo (Česká republika, Polsko, Portugalsko).	W1, W2 U1, U2, K1

Zůstatek kreditů ECTS		
Forma pracovního zatížení studentů		Počet hodin
Počet hodin s přímou účastí akademického pracovníka		
1.1	Účast na přednáškách	6
1.2	Účast na seminářích	
1.3	Účast na seminářích	14
1.4	Účast na laboratorních činnostech	
1.5	Účast na projektech	
1.6	Účast na konzultacích (2-3krát za semestr)	
1.7	Účast na konzultacích k projektu	
1.8	Účast na zkouškách/testech	2
1.9	Ostatní ...	
1.10	**Počet hodin strávených za přímé asistence akademických pracovníků (součet 1.1 - 1.9)**	22
1.11	**Počet ECTS kreditů, které student získal v hodinách vyžadujících přímou účast akademického pedagoga)**	1
Individuální práce studentů		
2.1	Individuální studium (včetně e-learningových přednášek)	25
2.2	Individuální příprava na semináře	10
2.3	Individuální příprava na test	

2.4	Individuální příprava na laboratorní výuku	
2.5	Příprava zpráv	
2.6	Realizace samostatně prováděných úkolů (projekty, dokumentace)	
2.7	Příprava na závěrečnou zkoušku/testy semináře	5
2.8	Příprava na závěrečnou zkoušku/testování přednášek	5
2.9	Další	
2.10	**Počet hodin individuální práce (součet 2.1 - 2.9)**	45
2.11	**Počet kreditů ECTS získaných studentem v rámci jednotlivých vzdělávacích aktivit**	1,5
Celková pracovní zátěž (h)		**67**
ECTS kredity za modul		**2,5**

Metody ověřování výsledků učení

Výsledek učení	**Formy kreditních tříd**								
	Ústní zkouška	Písemná zkouška	Částečný písemný úkol	Závěrečný písemný úkol (esej atd.)	Test	Design/prezentace	Nahlásit	Činnosti ve třídě	Ostatní ...
NOVINKY									
W1		x	x		x			x	
W2		x	x		x			x	
DOVEDNOSTI									
U1						x			
U2						x			
SOUTĚŽE									
K1								x	

Kritéria pro hodnocení kompetencí studentů
Minimální požadavky na tři skupiny výsledků učení, kterých musí student dosáhnout, aby předmět absolvoval, jsou uvedeny níže v syntetické podobě. Aby Student modul absolvoval, musí být všechny výsledky učení popsané v sylabu pozitivně ověřeny osobou (osobami), která modul vyučuje.

W - VĚDOMOSTI
Hodnocení:
Uspokojivý - Student si pamatuje a reprodukuje znalosti, které má v rámci modulu zvládnout.
Dobrý - Žák dodatečně interpretuje jevy / problémy a je schopen vyřešit typický problém.
Velmi dobře -Student je schopen řešit i složité problémy v daném oboru, je schopen syntetizovat, provést komplexní hodnocení, vytvořit práci, která je originální a inspirativní pro ostatní.

U - DOVEDNOSTI
Hodnocení:
uspokojivý - student zná podstatu činností a je schopen pod vedením akademického učitele provádět činnosti/řešit problémy související s obsahem modulu.
Dobrý - Student je schopen samostatně provádět činnosti / úkoly / řešit typické problémy související s obsahem modulu.
Velmi dobře - Student si plně osvojil schopnost / dovednost provádět činnosti / úkoly / problémy stanovené v obsahu modulu, a to i ve složitějších případech.

K - SOCIÁLNÍ KOMPETENCE

Hodnocení:
uspokojivě - student pasivně vstřebává obsah modulu, prokazuje schopnost soustředit se a naslouchat.
Dobrý - Žák se aktivně účastní výuky, vytváří hodnotové soudy podle kritérií přijatých v daném oboru, dokáže aktivně spolupracovat ve skupině.
Velmi dobře - Žák integruje postoje podle navrženého modelu, rozvíjí vlastní systém profesních a společenských hodnot, je schopen převzít odpovědnost za jednání skupiny, včetně vedení.

Forma pracovní zátěže studentů		Počet hodin
Počet hodin s přímou účastí akademického pracovníka		
1.1	Účast na přednáškách	6
1.2	Účast na seminářích	
1.3	Účast na seminářích	14
1.4	Účast na laboratorních činnostech	
1.5	Účast na projektech	
1.6	Účast na konzultacích (2-3krát za semestr)	
1.7	Účast na konzultacích k projektu	
1.8	Účast na zkouškách/testech	2
1.9	Ostatní ...	
1.10	**Počet hodin strávených za přímé asistence akademických pracovníků (součet 1.1 - 1.9)**	22
1.11	**Počet ECTS kreditů, které student získal v hodinách vyžadujících přímou účast akademického pedagoga)**	1

Individuální práce studentů		
2.1	Individuální studium (včetně e-learningových přednášek)	25
2.2	Individuální příprava na semináře	10
2.3	Individuální příprava na test	
2.4	Individuální příprava na laboratorní výuku	
2.5	Příprava zpráv	
2.6	Realizace samostatně prováděných úkolů (projekty, dokumentace)	
2.7	Příprava na závěrečnou zkoušku/testy semináře	5
2.8	Příprava na závěrečnou zkoušku/testování přednášek	5
2.9	Další	
2.10	**Počet hodin individuální práce (součet 2.1 - 2.9)**	45
2.11	**Počet kreditů ECTS získaných studentem v rámci jednotlivých vzdělávacích aktivit**	1,5
Celková pracovní zátěž (h)		**67**
ECTS kredity za modul		**2,5**

2. Základní materiály pro učitele

Definice (slovníček pojmů)

Přirozené právo *(ius naturale)* - existuje nezávisle na státu. Vzniká a rozvíjí se ve společnosti. Obecně zahrnuje soubor pravidel odpovídajících dosaženému stupni vývoje společnosti.
Pozitivní právo *(ius positivum)* - je uzákoněno státem nebo vládním systémem. Pozitivní právo je tedy předem dáno. Skládá se z předvídatelných pravidel, která jsou vynucována, tj. jejichž porušení je trestáno.
Právo - (neboli objektivní právo) - soubor právních norem jako obecně platných pravidel chování stanovených nebo uznaných a vynucovaných státem.
Právo - možnost právních subjektů chovat se tak, jak zaručuje právní norma. Právu obvykle odpovídá právní povinnost jiného právního subjektu.
Struktura právní normy - skládá se ze tří částí, kterými jsou **hypotéza, dispozice** a **sankce**.
Dispozitivní právní norma - vůbec nestanoví základní pravidlo chování nebo je stanoví pouze jako možnost. Stanovení pravidel ponechává na adresátech. Pokud tak adresáti neučiní, slouží pravidla v normě jako vodítko pro soudce, aby věděl, jak rozhodnout.
Kognitivní právní norma - stanoví platné pravidlo chování. Neponechává žádný prostor pro vůli adresáta.
Nárokové **normy** - právní normy výslovně formulují pouze nároky.
Závazné normy - právní normy výslovně formulují povinnost ve formě příkazu nebo zákazu.
Veřejnoprávní normy - právní normy platí tam, kde je vykonávána veřejná moc. Veřejnou moc vykonává stát prostřednictvím orgánů moci zákonodárné, výkonné a soudní. Veřejné právo chápeme jako oblast práva, kde jsou vztahy založeny na nerovnosti stran, kde jedna strana představuje veřejnou moc působící proti soukromým osobám prostřednictvím příkazů, zákazů a výkonu.
Soukromoprávní normy - právní normy se uplatňují v oblasti soukromého práva, tj. tam, kde jsou subjekty v rovném postavení a žádný z nich nemůže autoritativně rozhodovat o právech a povinnostech druhého. Subjekty upravují svá vzájemná práva a povinnosti prostřednictvím smluv a dohod.
Mezinárodní normy - právní normy upravují vztahy mezi státy nebo jejich národy, případně na úrovni Evropské unie.
Vnitrostátní normy - právní normy upravují vztahy mezi subjekty v rámci jurisdikce státu nebo obvykle na jeho území.
Hmotné právo - právní normy vymezují právní vztahy obecně a stanoví práva a povinnosti subjektů.
Procesní právo - právní normy upravují postup orgánů veřejné moci při aplikaci norem hmotného práva, jehož výsledkem může být vydání veřejnoprávního aktu.
Obecné právní normy se vztahují na celé území státu nebo Evropské unie. Dále se vztahují na všechny subjekty bez jakéhokoli omezení jejich časové působnosti.

Specifické normy - právní normy působí pouze na určitém území. Jinak - platí pouze pro určitou kategorii subjektů nebo po určitou dobu.
Účinnost právní normy - znamená, že dotyční adresáti mají práva a povinnosti z ní vyplývající.
Kyberprostor - lze definovat jako prostor kybernetických aktivit nebo jako prostor vytvořený informačními a komunikačními technologiemi, v němž se vytváří virtuální svět (nebo prostor) paralelní k prostoru reálnému.
Kyberprostor - digitální prostředí, které umožňuje vytváření, zpracování a výměnu informací a které se skládá z informačních systémů a služeb a sítí elektronických komunikací.
Kyberprostor - lze definovat dostupností a sledovatelností dat pro běžného uživatele.
Kyberprostor - je prostor skládající se ze tří vrstev: fyzické, logické a sociální.
Fyzická vrstva - zahrnuje pojem **geografická složka** a pojem **fyzické síťové prvky**.
Logická vrstva - obsahuje logické **prvky sítě, tj.** logická spojení mezi uzly sítě. Ta jsou realizována pomocí síťových komunikačních protokolů. Uzly mohou být počítače, telefony a další síťová zařízení.
Sociální vrstva - skládá se ze složek zvaných "**kybernetičnost"** a **osobnost**.
Definující standardy - jsou vytvářeny a zaváděny těmi, kteří mají pravomoc definovat prostředí informační sítě. V praxi se jedná o normy *sui generis,* které definují informační sítě jako takové. Existují ve vrstvách, které jsou na sobě vzájemně závislé.
Definující autority - jsou tvůrci definujících norem. Jedná se o subjekt, který svou činností vytváří pravidla logického systému, v němž orgán funguje.
Internet existuje pouze díky definujícím orgánům. Skládá se z. Žádná operace se neuskuteční bez účasti (provedení nebo zprostředkování provedení operace) definujícího orgánu.
Poskytovatel služeb - jakýkoli veřejný nebo soukromý subjekt, **který poskytuje uživatelům svých služeb možnost komunikovat prostřednictvím počítačového systému.**
Poskytovatel služeb - jakýkoli jiný subjekt, který zpracovává nebo ukládá počítačová data jménem komunikační služby nebo uživatelů takové služby.
Službou informační společnosti se rozumí jakákoli služba poskytovaná elektronicky na individuální žádost uživatele oznámenou elektronickými prostředky, obvykle poskytovaná za úplatu. Služba je poskytována elektronicky, pokud je přenášena prostřednictvím sítě elektronických komunikací a uživatel ji získává z elektronických zařízení pro ukládání dat.
Službou elektronických komunikací se rozumí služba, která je obvykle poskytována za úplatu a je založena na (úplném nebo převážném) přenosu signálů prostřednictvím sítě elektronických komunikací.
Veřejně dostupná služba elektronických komunikací - je služba elektronických komunikací, z jejíhož využívání není nikdo na počátku vyloučen.
Operátor - zajišťující nebo oprávněný zajišťovat veřejnou komunikační síť nebo přidružená zařízení je zákonem označován jako **operátor.**

Účastník - je každý, kdo uzavřel smlouvu o poskytování takové služby s podnikem poskytujícím veřejně dostupné služby elektronických komunikací.
Uživatel - je každý, kdo používá nebo požaduje veřejně dostupné služby elektronických komunikací.
Test proporcionality - je standardním právním nástrojem mezinárodních i ústavních (vnitrostátních) soudů při posuzování kolize právních norem, které slouží k ochraně ústavně zaručeného práva nebo veřejného zájmu, s jiným základním právem nebo svobodou.
Zásada vhodnosti - (fitness for purpose), podle níž **musí být opatření schopno dosáhnout zamýšleného účelu,** kterým je ochrana jiného základního práva nebo veřejného blaha.
Zásada nezbytnosti - stanoví **použití pouze nejekologičtějšího prostředku k dosažení zamýšleného účelu (zásahu do** základních práv a svobod) **z několika možných prostředků.**
Zásada proporcionality - (v užším smyslu) má za cíl zabránit **újmě na základním právu, která by byla nepřiměřená sledovanému cíli, tj.** opatření omezující základní lidská práva a svobody nesmí v případě střetu základního práva nebo svobody s veřejným zájmem svými negativními důsledky převážit pozitiva těchto opatření ve veřejném zájmu.
GDPR/RODO - Obecné nařízení o ochraně osobních údajů
Systém řízení bezpečnosti informací (**ISMS**)[2] - **je soubor zásad** určených k zachování důvěrnosti, integrity a dostupnosti informací prostřednictvím procesu řízení rizik a ujištění zúčastněných stran, že rizika jsou vhodně řízena.[3]
ISMS - je součástí procesů a celkového systému řízení organizace a je do něj integrován.
Cyklus PDCA - zkratka pro Plánuj-Dělej-Kontroluj-Dělej.
Varianta **OPDCA** - rozšiřuje původní model o fázi **pozorování, která** předchází fázi plánování.
Hodnocení rizik - označuje **celkový proces identifikace, analýzy a hodnocení rizik.**
Bezpečnostní politika - je soubor zásad a pravidel, které definují způsob zajištění ochrany aktiv**.**
Matice RACI (**RACI matrix) - zkratka pro responsible, accountable, consulted, informed (odpovědný, odpovědný, konzultovaný, informovaný).**
Subjekt podpory je technický pracovník, zaměstnanci a dodavatelé, kteří se podílejí na provozu, vývoji, správě nebo zabezpečení systému ICT.
Podkladovým aktivem jsou informace nebo služby zpracovávané nebo poskytované systémem ICT.
BCM - zkratka pro řízení kontinuity provozu.
Prostory - budova nebo jiný uzavřený prostor.
Oprávnění znamená právo přístupu k nějakému prostředku (obvykle počítači nebo komunikačnímu systému, aplikaci atd.) V praxi se jedná o nástroj pro "správu uživatelů a skupin" a nástroj pro nastavení oprávnění k souborům a adresářům. Tyto nástroje jsou proprietární součástí všech standardních operačních systémů.

[2] Dále jen **ISMS**
[3] Srov. zavedení ČSN ISO/IEC 27001

Centrální server **AAA -** zkratka pro Authentication, Authorisation, Accounting.
SIEM - zkratka pro správu bezpečnostních incidentů a událostí.
Kryptografie (šifrování) - vědní obor zabývající se transformací srozumitelných informací do podoby, která je pro příjemce nesrozumitelná, pokud nemá klíče, jimiž by mohl informace dešifrovat.
Nařízení GDPR - je **obecný právní rámec pro ochranu osobních údajů, který** je platný a účinný v celé EU a v některých případech i mimo ni.
Osobní údaje - jsou **veškeré informace týkající se identifikované nebo identifikovatelné fyzické osoby**. Identifikovatelná fyzická osoba je osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na identifikátor, jako je jméno, identifikační číslo, lokační údaje, online identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.
Osobní údaje jsou **veškeré informace** (např. obrazové, písemné, ústní, digitální, genetické, lékařské atd.), které **jsou spojeny** (prostřednictvím obsahu - např. jméno, adresa, pozice, e-mail atd.) **se subjektem** údajů**.**[4]
"Objektivní kritérium" - znamená, že údaje, jako jsou **IP adresy, by mohly být považovány za osobní údaje** zpracovávané poskytovateli služeb, kteří nejsou poskytovateli připojení (např. provozovatelem webových stránek), **i když by konkrétního uživatele mohla identifikovat pouze třetí strana** (typicky poskytovatel připojení).
"**Relativní**" **kritérium -** znamená, že **IP adresy by mohly být považovány za osobní údaje pro připojení k ISP,** protože umožňují poskytovateli zjistit totožnost uživatele, **ale již ne pro stránky ISP, které ve skutečnosti mají pouze informace o IP adrese a neznají jméno návštěvníka**.
Zpracováním osobních údajů se rozumí **operace nebo soubor operací, které** se provádějí s osobními **údaji** nebo soubory osobních údajů, **ať už automatizovaně, nebo neautomatizovaně,** jako je shromažďování, zaznamenávání, uspořádávání, organizování, uchovávání, přizpůsobování nebo pozměňování, vyhledávání, nahlížení, používání, sdělování přenosem, šíření nebo jiné zpřístupňování, seřazování nebo kombinování, omezování, výmaz nebo zničení.
DPIA - posouzení vlivu na ochranu osobních údajů
DPIA - je nástrojem, který se používá v případech, kdy **je pravděpodobné, že** určitý typ **zpracování, zejména s využitím nových technologií, bude vzhledem k** povaze, rozsahu, kontextu a účelům zpracování představovat **vysoké riziko pro práva a svobody fyzických osob.**
RIR - zkratka pro **regionální internetový** registr.
LIR - zkratka pro **místní internetový** registr.

<u>Klíčové citace z online materiálů:</u>

[4]Podle čl.4 odst.1 GDPR je **subjektem údajů** identifikovaná nebo identifikovatelná **fyzická osoba**.**Subjekt údajů může být identifikován:**

- **přímo,**
- **nepřímo (např. zvýraznění atd.)**

- Právo je jedním z nejdůležitějších nástrojů stabilizace společenských vztahů a regulace společnosti.
- Právo je jednou z jeho možných regulací v podobě nedokonalých normativních konstrukcí, kde více než jinde platí pravidlo, že se nepřekrývá reálné chování, tedy to, co se v online prostředí skutečně realizuje, a normativní chování, tedy to, co by mělo být (z vůle regulátora i naší). Realita internetu a jeho normativní regulace jsou tedy dvě relativně samostatné kategorie. Tento předpoklad nebude zpochybněn ani v této publikaci. Naopak, bude jedním z jejích pilířů
- Vlastní pojem práva je poměrně obtížné definovat, neboť se jedná o multidisciplinární fenomén, který nelze vymezit jedinou definicí:
- **Přirozené právo** *(ius naturale)* existuje nezávisle na státu. Vzniká a rozvíjí se ve společnosti. Obecně zahrnuje soubor pravidel odpovídajících stupni vývoje, kterého společnost dosáhla.
- **Pozitivní právo** *(ius positivum)*. Toto právo vydává stát nebo vládní systém. Pozitivní právo je tedy předem dáno. Skládá se z předvídatelných pravidel, která jsou vymáhána, tj. jejichž porušení je trestáno.
- **Právem** (neboli objektivním právem) se rozumí soubor právních norem jako obecně platných pravidel chování stanovených nebo uznaných a vynucovaných státem.
- **Oprávnění (právo) -** je možnost právních subjektů chovat se tak, jak zaručuje právní norma. Oprávnění obvykle odpovídá právní povinnosti jiného právního subjektu. Prohlášení subjektu, že "toto je moje právo", je v tomto smyslu právní.
- **Právní norma** je obecně platné pravidlo chování, které upravuje práva a povinnosti subjektů. Toto pravidlo chování je vyjádřeno v konkrétní právní formě uznané státem (nebo Evropskou unií) a jeho dodržování je zajištěno vymáháním ze strany státu.

- Právní normy lze rozdělit podle různých kritérií. Mezi ně patří zejména:

  1. *Povaha pravidel stanovených právní normou.* Vzhledem k povaze pravidel se právní normy dělí na:
  - Dispozitivní. Dispozitivní právní norma nestanoví základní pravidlo chování vůbec nebo je stanoví pouze jako možnost. Stanovení pravidel ponechává na adresátech. Pokud tak adresáti neučiní, slouží pravidla obsažená v normě jako vodítko pro soudce, aby věděl, jak rozhodnout. Dispozitivní normy se nejčastěji používají v občanském právu nebo v občanskoprávních vztazích, které umožňují větší variabilitu při řešení různých situací (samoregulace).
  - Kogentní (kategorická).Kogentní právní norma stanoví závazné pravidlo chování. Neponechává prostor pro libovůli adresáta.

- **Kyberprostor** je:
    - kybernetický akční prostor, tj. prostor vytvořený informačními a komunikačními technologiemi, v němž se vytváří virtuální svět (nebo prostor) paralelní k tomu reálnému.
    - digitální prostředí, které umožňuje tvorbu, zpracování a výměnu informací a které se skládá z informačních systémů a služeb a sítí elektronické komunikace.
    - prostor skládající se ze tří vrstev: fyzické, logické a sociální.

- **Charakteristickými rysy kyberprostoru jsou** jeho **decentralizace, globalizace, otevřenost, množství informací, interaktivita** a možnost uživatele ovlivňovat názory. Důležitým atributem kyberprostoru je, že v něm hrají zásadní roli technologie a související služby. V poslední době je stále jasnější, že projevy virtuálního světa mohou mít a mají důsledky v reálném světě.

- Jednu z účinnějších definic *kyberprostoru lze* nalézt v dokumentu *Cyberspace Operations: Concept Capability Plan 2016-2028,* který definuje **kyberprostor jako prostor skládající se ze tří vrstev:** [5]

[5] TRADOC. Cyberspace Operations: Concept Capability Plan 2016-2028 [online]. [cit. 18. 2. 2018], s. 8-9. Dostupné z: www.fas.org/irp/doddir/army/pam525-7-8.pdf?

- fyzické,
- logické,
- Sociální oblast.

- **Kyberprostor lze také definovat podle dostupnosti a sledovatelnosti dat pro běžného uživatele.** Podle tohoto dělení lze kyberprostor rozdělit na služby a data přístupná prostřednictvím internetu, služby a data přístupná pouze v rámci specifických sítí a zařízení a služby a data záměrně skrytá a přístupná pomocí speciálních nástrojů.

Pro tyto kategorie se obvykle používají následující názvy:
- Povrchový web
- Hluboký web
- Temný web

- **Definiční normy** vytvářejí a zavádějí subjekty oprávněné definovat prostředí informační sítě. V praxi se jedná o normy *sui generis,* které definují informační sítě jako takové. Existují ve vrstvách, které jsou na sobě vzájemně závislé
- **Definující autority** jsou tvůrci definujících norem. Je to subjekt, který svým působením vytváří pravidla logického systému, v němž orgán funguje.
- Největším **určujícím subjektem,** i když to není subjekt, který vytváří pravidla logického systému, **je uživatel jako takový**.
- Pojem poskytování **elektronickými prostředky je definován ve** směrnici Evropského parlamentu a Rady (EU) 2015/1535 v čl. 1 písm. b) bodě ii), kde je definován jako služba, která je původně odeslána a v místě určení přijata pomocí elektronického zařízení pro zpracování (včetně digitální komprese) a uchovávání dat.
- **Individuální požadavek uživatele** znamená, že se musí jednat o aktivní akci uživatele.
- Pro stanovení jednotlivých práv a povinností poskytovatelů připojení je nutné rozdělit tyto poskytovatele do dvou skupin - **veřejné a neveřejné**. Na obě skupiny poskytovatelů připojení se vztahuje zákon o některých službách informační společnosti, avšak na veřejné poskytovatele připojení se vztahuje také zákon o elektronických komunikacích, který vymezuje další práva a povinnosti těchto poskytovatelů
- Podle § 6 ACISS **není poskytovatel připojení povinen** dohlížet na obsah přenášených informací **ani** aktivně zjišťovat, zda jsou přenášené informace protiprávní.
- **Služba elektronických komunikací** [§ 2 písm. n) zákona o elektronických komunikacích[6]]. Podle § 2 písm. n) EÚD se tímto pojmem rozumí služba, která je obvykle poskytována za úplatu a je založena na (úplném nebo převážném) přenosu signálů prostřednictvím sítě elektronických komunikací.
- **Veřejně dostupná služba elektronických komunikací** [§ 2 písm. o) ECA]. Tato služba je službou elektronických komunikací, z jejíhož využívání není nikdo předem vyloučen.
- **Podnik, který** zajišťuje nebo je oprávněn zajišťovat veřejnou komunikační síť nebo přiřazená zařízení, se v tomto zákoně označuje jako **operátor** [§ 2 písm. e) ZEK].
- **Účastníkem** [odst. 2 písm. a) ZEK] je každý, kdo uzavřel smlouvu o poskytování takové služby s podnikem poskytujícím veřejně dostupné služby elektronických komunikací.
- **Uživatel** je každý, kdo používá nebo požaduje veřejně dostupnou službu elektronických komunikací.
- **Test proporcionality** je standardním právním nástrojem mezinárodních i ústavních (vnitrostátních) soudů při posuzování kolize právních norem, jejichž cílem je ochrana ústavně zaručeného práva nebo veřejného zájmu, s jiným základním právem nebo svobodou.

[6] Dále jen EÚD

- **Systém řízení bezpečnosti informací** (**ISMS**)[7] **je soubor zásad určených k** zachování důvěrnosti, integrity a dostupnosti informací prostřednictvím procesu řízení rizik a ujištění zúčastněných stran, že rizika jsou vhodně řízena.[8]
- Řešení ISMS vyžaduje systémový a komplexní přístup, který respektuje zásady a prvky celého životního cyklu kybernetické bezpečnosti. Systém řízení ISMS je založen na Demingově cyklu neboli **cyklu PDCA** (**Plan-Do-Check-Act**).
- Z hlediska občanského práva může být majetkem **hmotná** věc (budova, počítačový systém, sítě, energie, zboží atd.) nebo **nehmotná** věc (informace, znalosti, data, programy atd.).
- Přínosem může být také **kvalita (např.** dostupnost a funkčnost systému a dat apod.) nebo **dobré jméno,** pověst apod.
- **Lidé** (uživatelé, správci atd.) jsou díky svým znalostem a zkušenostem přínosem i z hlediska kybernetické bezpečnosti.
- **Subjekt podpory** je technický pracovník, zaměstnanci a dodavatelé, kteří se podílejí na provozu, vývoji, správě nebo zabezpečení systému ICT.
- **Podkladovým aktivem** jsou informace nebo služby zpracovávané nebo poskytované systémem ICT.
- Řízení kontinuity činností (**BCM)** je proces založený na identifikaci klíčových prvků (systémů a procesů) v organizaci a následném zavedení procesů a postupů, které zajistí kontinuitu nebo obnovu těchto prvků na předem stanovené úrovni, na které bude ještě možné plnit hlavní úkoly organizace.
- Termín **perimetr** fyzické **bezpečnosti** označuje vymezený prostor nebo hranice tohoto prostoru. Takovým prostorem může být například soubor prostor, samotný areál nebo jeho část.
- **Prostory** jsou budova nebo jiný uzavřený prostor.
- **Hranicí areálu** se rozumí stavební přepážka, fyzická překážka (plot) nebo jiná viditelně vymezená hranice pozemku.
- **Zabezpečeným prostorem** se rozumí prostor v budově, který je stavebně nebo jinak viditelně oddělen.
- Pojem **oprávnění** znamená právo přístupu k jakémukoli prostředku (obvykle IT nebo komunikačnímu systému, aplikaci atd.) V praxi se jedná o nástroj pro "správu uživatelů a skupin" a nástroj pro nastavení oprávnění k souborům a adresářům.
- V rámci fyzické bezpečnosti musí někteří správci provádět **penetrační testy** systému ICT se zaměřením na důležitá aktiva, a to:
    - před uvedením do provozu a
    - v důsledku podstatné změny.
- V rámci zabezpečení aplikací podnik také zajišťuje, aby aplikace, informace a transakce byly vždy chráněny před:
    - neoprávněné jednání,
    - odmítnutí plnění.
- Hodnota rizika se nejčastěji vyjadřuje jako funkce dopadu, hrozby a zranitelnosti. Pro vlastní hodnocení rizika lze použít například následující funkci:

  Riziko = dopad * hrozba * zranitelnost

- Obecné nařízení o ochraně osobních údajů (EU) 2016/679 neboli GDPR/ RODO[9] je jedním z nejdůležitějších mezinárodních právních dokumentů, který se přímo týká problematiky kybernetické bezpečnosti, i když není primárně zaměřen na oblast informačních a komunikačních technologií.

GDPR ≠ IT + software.

[7] Dále jen **ISMS**
[8] Viz zavedení normy ISO/IEC 27001.
[9] [online]. Dostupné z: http://eur-lex.europa.eu/legal-content/

- **Osobní údaje jsou většinou zveřejňovány na sociálních sítích,** které ze své podstaty takové zveřejnění předpokládají a v podmínkách zakotvují zásady, podle nichž se s těmito údaji nakládá.
- Podle čl.4 odst.1 GDPR/RODO jsou osobními údaji "**veškeré informace týkající se identifikované nebo identifikovatelné fyzické osoby**.
- Podle čl. 4 odst. 2 nařízení RODO se zpracováním osobních údajů rozumí **jakákoli operace nebo** soubor **operací s osobními údaji** nebo soubory osobních údajů, které jsou prováděny automatizovaně či **nikoli,** jako je shromažďování, zaznamenávání, uspořádávání, organizování, uchovávání, přizpůsobování nebo pozměňování, vyhledávání, nahlížení, používání, sdělování přenosem, šíření nebo jiné zpřístupňování, seřazování nebo kombinování, omezování, výmaz nebo zničení.
- Jednou z oblastí, kterou GDPR výslovně řeší, je **bezpečnost zpracování osobních údajů**.
- Posouzení vlivu na ochranu osobních údajů (**DPIA)** je nástroj, který se používá v případech, kdy určitý typ **zpracování, zejména s využitím nových technologií, s ohledem** na povahu, rozsah, kontext a účely zpracování, **pravděpodobně představuje vysoké riziko pro práva a svobody fyzických osob**. Jedná se o nástroj, který může správcům pomoci identifikovat potenciální rizika spojená se zpracováním osobních údajů a zavést vhodná opatření.
- Posouzení vlivu na ochranu osobních údajů by mělo zahrnovat:
    - popis plánovaných zpracovatelských operací,
    - posouzení nezbytnosti a vhodnosti opatření z hlediska cíle (**test proporcionality)**,
    - posouzení rizik pro práva a svobody subjektů,
    - plánovaná opatření k řešení těchto rizik, včetně ochranných opatření, bezpečnostních opatření atd.
- Digitální stopy lze na základě toho, zda je uživatel může ovlivnit, obecně rozdělit **na stopy,** které **lze ovlivnit (aktivní), a na ty, které ovlivnit nelze (pasivní).**
- Ve výchozím nastavení není IP adresa anonymní a počítačový systém ji používá jako jeden ze svých identifikátorů při komunikaci s jinými počítačovými systémy. IP adresy jsou přidělovány hierarchicky, přičemž dominantní roli hraje **organizace ICANN,** která rozděluje reálný svět do oblastí spravovaných **regionálními** internetovými **registry** (**RIR)**.
- Regionální registry dále rozdělují přidělené IP rozsahy mezi **místní** internetové registry (**LIR)**. Místním registrem je obvykle poskytovatel internetového připojení, ať už veřejný, nebo neveřejný. Tento registr pak může sdílet svůj rozsah IP adres například s částmi své organizace nebo jinými subjekty.

3. Během výuky

<u>Několik nápadů na aktivity:</u>

WORKSHOPY

1. Vymezení působnosti práva v kyberprostoru (hranice, možnosti atd.).
2. Soukromoprávní a veřejnoprávní odpovědnost za jednání uživatele nebo společnosti v online prostředí.
3. Charakteristika a definice jednotlivých poskytovatelů internetových služeb a jejich práv a povinností ve vztahu ke kybernetické bezpečnosti.
4. ISMS a vztah k zákonu o kybernetické bezpečnosti.
5. Základní práva a povinnosti jednotlivých subjektů ze směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních pro vysokou společnou úroveň bezpečnosti sítí a informačních systémů v Unii, a to i z vnitrostátních právních předpisů.
6. Uplatňování práv a povinností GDPR/RODO v kyberprostoru.

7. Praktická analýza podmínek vzorových smluv o ochraně osobních údajů poskytovatelů internetových služeb.

KONTROLNÍ OTÁZKY

1.

- Jaký je zákon?
- Co je to právní norma a jak se dělí?
- Co je to kyberprostor?
- Z jakých vrstev se skládá kyberprostor?
- Platí právo v kyberprostoru, a pokud ano, jaké právní normy se na něj vztahují?
- Jak lze právo uplatňovat v kyberprostoru, včetně možných sankcí nebo jiných opatření?
- Uveďte několik příkladů uplatňování práva v kyberprostoru.
- Definice ISMS.

2.

- Definujte PSI.
- Jak jsou poskytovatelé internetových služeb rozděleni? Podle jakých kritérií?
- Jaké jsou povinnosti poskytovatelů internetových služeb?
- Co je určující standard?
- Kdo je určujícím orgánem a jaká je jeho úloha?
- Co je to uchovávání dat?

3.

- Co je cyklus PDCA a jaké je jeho použití?
- Jaké prvky lze zahrnout do fyzické bezpečnosti?
- Co je to: Řízení kontinuity podnikání?
- Definujte hrozbu.
- Definujte riziko.
- Definujte dopad.
- Definujte zranitelnost.
- Definujte aktiva.
- Co je aktivum, co jsou aktiva?

4.

- Jaká je územní působnost GDPR?
- Co jsou osobní údaje?
- Je IP adresa osobní údaj?

- Jaké jsou povinnosti správce osobních údajů?
- Co se rozumí zpracováním osobních údajů?
- Co znamená posouzení vlivu na ochranu osobních údajů?

5.

- Definujte pojem "digitální stopa".
- Jaký je rozdíl mezi digitálními otisky?
- Z jakých složek se skládá pasivní digitální stopa?
- Co je to LIR?
- Jaké informace o uživateli nese IP adresa?
- Co je to smlouva EULA?

Práce ve dvojicích/skupinách

- **Dvojice - miniprojekt**
  Studenti si ve dvojicích vyberou jedno z probíraných témat. Zapíší své závěry a představí je ostatním. Po prezentaci si ostatní studenti připraví doplňující otázky pro prezentující skupinu.

- **Myšlenková mapa**
  Studenti si ve dvojicích vyberou jedno z probíraných témat a vytvoří myšlenkovou mapu, kterou poté popíší ostatním studentům v krátké prezentaci.

- **Klíčová slova**
  Studenti ve dvojicích samostatně vyberou klíčová slova ze slovníčku.

Definice těchto slov napíší na proužky papíru. Proužky otočí prázdnou stranou nahoru. Jeden student si vybere proužek, přečte definici a druhý student hledá odpovídající klíčové slovo.
nebo
Studenti si na papír napíší několik klíčových slov ze slovníčku. Kartičky otočí prázdnou stranou nahoru. Jeden student si vezme první kartičku a řekne, co dané slovo znamená. Druhý student klíčové slovo hádá.

- 10 klíčových slov
  Studenti si vyberou 10 klíčových slov souvisejících s vybraným tématem. Těchto 10 klíčových slov předají ostatním dvojicím. Dvojice napíší text, který musí obsahovat všechna klíčová slova. Jedna věta může obsahovat pouze jedno klíčové slovo. Text se tedy skládá minimálně z 10 vět.

- Panelová diskuse

  Studenti si vyberou 3 řečníky. Každý řečník si vybere jedno téma, o kterém bude diskutovat. Ostatní studenti kladou otázky k tématům. Každý mluvčí může použít typ odpovědi -PRAVDA X NEPRAVDA. Za každou pravdivou odpověď získá student bod, např. znamená GDPR General Data Protection Regulation? - PRAVDA X NEPRAVDA.

4. Internetové zdroje

Viz bibliografie.

5. Další otázky/testy

VYBERTE SPRÁVNOU ODPOVĚĎ:
(Správná odpověď byla podtržena)

1. _____ je stanovena státem nebo systémem vlády, a je tedy předem daná. Skládá se z předvídatelných pravidel, která jsou vynucována, tj. jejich porušení je trestáno.

   a) Pozitivní právo
   b) Přirozené právo
   c) Subjektivní právo
   d) Objektivní právo

2. _____představuje obecně platné pravidlo chování, které upravuje práva a povinnosti subjektů.

   a) Právní norma
   b) Právní právo
   c) Právní norma
   (d) Právní linka

3. _____ - pravidlo chování upravuje společenské vztahy se závaznou platností.

   (a) konečné rozhodnutí
   (b) právně vedoucí
   (c) právně odůvodněné
   (d) právně závazné

4. Standardní struktura právní normy se skládá ze tří částí, které jsou _____.

   (a) hypotéza, dispozice a sankce
   (b) předvídání, likvidace a sankce
   (c) hypotéza, porušení a sankce
   (d) hypotéza, dispozice a sankce

5. _____ je vyjádřením důsledků porušení právní povinnosti vyplývající z dispozice právní normy.

   a) Repatriace
   (b) Posudek
   (c) Sankce

(d) Revize

6. Norma _____ vůbec nespecifikuje základní pravidlo chování nebo ho definuje pouze jako možnost. Stanovení pravidel je ponecháno na adresátech. Pokud tak adresáti neučiní, slouží ustanovení v normě jako vodítko pro soudce při rozhodování.

   (a) logické
   (b) dispozitivní
   (c) kategorické
   (d) významné

7. _____ právní normy upravují vztahy mezi subjekty v rámci jurisdikce státu nebo obvykle na jeho území.

   a) Veřejnost
   (b) Mezinárodní
   c) Soukromé
   d) Národní

8. _____ právní normy platí pro celé území státu nebo Evropské unie. Navíc se vztahují na všechny subjekty bez jakéhokoli omezení jejich časové působnosti.

   (a) Mezinárodní
   b) Vnitrostátní
   c) Věcné
   d) Občanské právo

9. Kyberprostor lze také definovat jako prostor kybernetických aktivit nebo jako prostor vytvořený informačními a komunikačními technologiemi, v němž se vytváří _____svět (nebo prostor) paralelní k reálnému prostoru.

   (a) digitální
   (b) skutečné
   (c) virtuální
   (d) aktuální

10. Kyberprostor lze také definovat podle dostupnosti a _____ dat pro běžného uživatele.

    (a) účinnost
    (b) účinnost
    (c) výkonnost
    (d) sledovatelnost

11. Zásada_____ znamená, že k dosažení zamýšleného účelu (zásahu do základních práv a svobod) je třeba použít z několika možných prostředků pouze ten, který je nejšetrnější k životnímu prostředí.

    (a) nutnost

    (b) přiměřenost

    (c) odbornost

    (d) vhodnost

12. Co znamená zkratka ISMS?

    (a) Bezpečný systém správy informací

    (b) Systém řízení bezpečnosti informací

    (c) Systematická správa zabezpečených informací

    (d) Tým pro bezpečnost systémových informací

13. Bezpečnostní politika je soubor zásad a pravidel, které _____politiky zajišťují/-e/-u ochranu aktiv.

    (a) určit

    (b) ovlivňují

    (c) zabránit

    (d) vliv

14. Termín _____ znamená právo na přístup k jakémukoli aktivu (obvykle informačnímu nebo komunikačnímu systému, aplikaci atd.).

    (a) aplikace
    (b) licence
    (c*) povolení)*
    (d) projít

15. Co znamená zkratka DPIA?

    a) Posouzení dopadu povolených údajů
    b) Posouzení vlivu na ochranu osobních údajů
    (c) Posouzení dopadu na údaje
    (d) Hodnocení dopadu slibných údajů

Bibliografie

ANGWIN, Julia. *Seznamte se s online sledovacím zařízením, které je prakticky nemožné zablokovat.* [online]. [citováno 10. 6. 2016].

BARLOW, Perry John. *Deklarace nezávislosti kyberprostoru.* [online]. [cit. 23.09.2014]. Dostupné z: https://www.eff.org/cyberspace-independence.

CAETANO, Lianne. *Jsou vaše aplikace příliš sdílené? Zpráva o bezpečnosti mobilních zařízení za rok 2014 říká vše.* [online]. [citováno 10. 4. 2015]. Dostupné z: https://blogs.mcafee.com/consumer/mobile-security-report-2014/.

CNN o pedofilním sexu v Second Life. [online]. [citováno 18.06.2009]. Dostupné z: http://www.youtube.com/watch?v=AQM-SiiaipE
Současná světová populace. [online]. [cit. 10.08.2015]. Dostupné z: http://www.worldometers.info/world-population/.

Zajímavé statistiky o mobilních strategiích pro digitální transformaci. [online]. [cit. 15. 7. 2016]. Dostupné z: http://www.smacnews.com/digital/interesting-statistics-on-mobile-strategies-for-digital-transformations/

Uchovávání údajů je v současné podobě protiústavní. [online]. [cit. 16. 7. 2016]. Dostupné z: https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2010/bvg10-011.html?nn=5404690

Digitální, sociální a mobilní technologie ve světě v roce 2015. [online]. [citováno 09/08/2015]. Dostupné z:http://www.slideshare.net/wearesocialsg/digital-social-mobile-in-2015?ref=http://wearesocial.net/blog/2015/01/digital-social-mobile-worldwide-2015/

ENGLEHARDT, Steven a Ardvin NARAYANAN. *Online sledování: Měření a analýza 1 milionu stránek.* [online]. [cit. 05.08.2016]. Dostupné z: http://randomwalker.info/publications/OpenWPM_1_million_site_tracking_measurement.pdf.

Facebook vás brzy bude moci identifikovat na každé fotografii. [online]. [citováno 09.08.2015]. Dostupné z: http://news.sciencemag.org/social-sciences/2015/02/facebook-will-soon-be-able-id-you-any-photo

FBI využívá zranitelnost ve Flashi k prolomení zabezpečení sítě Tor. [online]. [cit. 23. 7. 2016]. Dostupné z: https://nordvpn.com/blog/fbi-exploits-flash-vulnerability-to-breach-tor-network-security/.

První dodatek. [online]. [cit. 10. 7. 2016]. Dostupné z: https://www.law.cornell.edu/constitution/first_amendment.

Německý Bundestag schválil nový zákon o uchovávání údajů. [online]. [cit. 16. 7. 2016]. Dostupné z: http://www.gppi.net/publications/global-internet-politics/article/german-bundestag-passes-new-data-retention-law/

HAINES, Lester. *Online hráč pobodaný "ukradeným" kybernetickým mečem.* [online]. [citováno 10. 3. 2006]. Dostupné z: http://www.theregister.co.uk/2005/03/30/online_gaming_death/

HUSOVEC, Martin. *Zodpovednosť na Internete podľa českého a slovenského práva*. Praha: CZ.NIC, 2014. ISBN: 978-80-904248-8-3, s. 101-102.

Cenzura na internetu. [online]. [cit. 10.08.2016]. Dostupné z: http://www.deliveringdata.com/2010_10_01_archive.html.

Historie internetu v 80. letech [online]. [citováno 07.06.2016]. Dostupné z: http://www.computerhistory.org/internethistory/1980s/.

JOHNSON, David R. a David POST. *Vzestup práva v kyberprostoru.* [online]. [cit. 10. 7. 2016].

KOLOUCH, Jan a Andrea KROPÁČOVÁ. Odpovědnost za vlastní zařízení a data a aplikace v něm uložené. In: *Pokroky v informační vědě a aplikacích, svazek I: Sborník 18. mezinárodní konference o počítačích (součást CSCC '14).* [B.m.], c2014, s. 321-324. Recent Advances in Computer Engineering Series, 22. ISBN 978-1-61804-236-1 ISSN 1790-5109.

KOLOUCH, Jan. *Kyberkriminalita.* Praha: CZ.NIC, 2016, s. 78 a násl. a s. 109 a násl.

Přední sociální sítě na světě, duben 2016, pořadí podle počtu aktivních uživatelů (v milionech) [online]. [citováno 10.08.2015]. Dostupné z: http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

LESSIG, Lawrence. *Code v. 2. p.* 6 Dostupné v plném znění (ang) [online]. [cit.13/03/2008]. Dostupné na: http://pdf.codev2.cc/Lessig-Codev2.pdf

MAISNER, Martin aBarbora VLACHOVÁ. *Zákon o kybernetické bezpečnosti. Komentář.* Praha: Wolters Kluwer, 2015. s. 85

MATEJKA, Ján. *Internetová jakoobjektpráva: hledánírovnováhyautonomie a soukromí.* Praha: CZ.NIC, 2013. ISBN 978-80-904248-7-6 s. 25

Vnitrostátní právní námitky proti směrnici o uchovávání údajů. [online]. [cit. 16. 7. 2016]. Dostupné na: https://eulawanalysis.blogspot.cz/2014/04/national-legal-challenges-to-data.html.

Cyklus PDCA. [online]. [cit. 06/07/2018]. Dostupné z: https://www.creativesafetysupply.com/glossary/pdca-cycle/.

PETERKA, Jiří. *Uchovávatprovozní a lokalizačníúdajenámuž EU nenařizuje. My to v tom ale pokračujeme.* [online]. [citováno 10. 11. 2015]. Dostupné z: http://www.earchiv.cz/b14/b0428001.php3

REED, Chris. *Internetové právo*. Cambridge: Cambridge University Press, 2004, s. 218.
Regionální online registry. [online]. [citováno 04.08.2015]. Dostupné z: https://*www.nro.net/about-the-nro/regional-internet-registries.*

ROSER, Christoph. *Mnoho chutí PDCA.* [online]. [cit. 06/07/2018]. Dostupné z: https://www.allaboutlean.com/pdca-variants/.

SMITH, Craig. *Podle čísel: 100 úžasných statistik a faktů z vyhledávače Google.* [online]. [cit. 04/08/2016]. Dostupné z: http://expandedramblings.com/index.php/by-the-numbers-a-gigantic-list-of-google-stats-and-facts/.

Soudní dvůr Evropské unie. Tisková zpráva č. 54/14, 8. dubna 2014. Rozsudek ve spojených věcech C-293/12 a C-594/12 [online]. [citováno 15. 7. 2016]. Dostupné z: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054cs.pdf.

Stanovisko generálního advokáta Pedra Cruze Villalóna. Věc C-293/12 a C-594/12 [online]. [cit. 15/07/2016]. Dostupné v: Sbírka zákonů: http://curia.europa.eu/juris/document/document.jsf?text=&docid=145562&pageIndex=0&doclang=CS&mode=req&dir=&occ=first&part=1&cid=727954

Stanovisko generálního advokáta SAUGMANDSGAARDA ØE ze dne 19. 7. 2016. Ve spojených věcech C-203/15 a C-698/15 [online]. [citováno 10. 8. 2016]. Dostupné na adrese: http://curia.europa.eu/juris/document/document.jsf?text=&docid=181841&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=111650

Povrchový web, hluboký web, temný web - jaký je mezi nimi rozdíl. [online]. [citováno 20. 7. 2016]. Dostupné z: https://www.cambiaresearch.com/articles/85/surface-web-deep-web-dark-web----whats-the-difference.

Modul 3

Detekce
a prevence
kybernetických hrozeb

1. Úvod

1.1 Shrnutí kurzu

Kurz se zpočátku zaměřuje na přehled základních právních norem kyberkriminality. Pro pochopení celé problematiky je rovněž nezbytné porozumět pojmu kyberkriminalita. Významná část kurzu se zabývá klasifikací kyberkriminality. V kurzu jsou rozebrány jednotlivé kybernetické trestné činy, které jsou velmi podrobně popsány. Hlavní část kurzu je věnována kybernetickým útokům a jejich postihům.

1.2 Cíle kurzu

Studenti se seznámí s právními normami upravujícími kyberkriminalitu. Cílem předmětu je seznámit studenty s problematikou kybernetických útoků, které mohou mít znaky protiprávního jednání, a s možnou právní kvalifikací takového jednání. Hlavní částí kurzu je identifikace forem a způsobů páchání kyberkriminality. Kurz se zaměřuje také na spam, podvody, hoaxy a botnety. Dále se studenti budou zabývat kybernetickými útoky, konkrétně těmi, které se týkají financí (pharming, spearphishing, mobilní phishing), ale také útoky týkajícími se společnosti (kyberšikana, stalking, sexting, kybergrooming atd.). Důležitým obsahem tohoto modulu je prevence těchto negativních jevů.

1.3 Obsah kurzu

Jednotlivé přednášky seznamují studenty s právními normami upravujícími kyberkriminalitu. Dále se studenti seznámí se sociálním inženýrstvím, spamem, podvodem, hoaxem a botnetem. Během přednášek jsou studenti seznámeni s různými typy kybernetických útoků, jako je hacking, cracking, malware, ransomware. Zmíněny jsou nejen kybernetické útoky, jako jsou útoky zaměřené na finance (phishing, pharming, spearphishing, mobile phishing), ale také sociální kybernetické útoky (kyberšikana, stalking, sexting, kybergrooming atd.).

1.4 Cíle učení

1) Úvod do terminologie kyberkriminality
2) Seznámení se s vnitrostátními předpisy o kyberkriminalitě
3) Seznámení se s mezinárodními předpisy o kyberkriminalitě
4) Pochopení významu sociálního inženýrství v kontextu kybernetických útoků.
5) Povědomí o projevech kyberkriminality
6) Porozumění kybernetickým útokům

1.5. Potřebné vybavení a materiály

Detekce a prevence kybernetických útoků - k dispozici online

1.6 Sylabus

Výsledek učení	Student, který úspěšně absolvuje tento modul, bude znát/umět následující.
NOVINKY	
W1	Student získá obecný přehled o vnitrostátních a mezinárodních právních normách, které definují nezákonné činnosti v kyberprostoru.
W2	Student se seznámí se základní technickou terminologií, která se týká kybernetických útoků, kybernetických incidentů, kybernetické kriminality atd. Bude schopen rozlišit, která právní norma nebo zvláštní ustanovení se na daný útok vztahují a proč.
DOVEDNOSTI	
U1	Po absolvování kurzu bude student schopen identifikovat základní kybernetické útoky, jejich modus operandi, způsobené následky atd.
U2	Na základě výše uvedené identifikace bude student schopen aplikovat konkrétní právní případy na dané porušení. Student bude schopen přijmout základní preventivní opatření k případné eliminaci negativního chování v budoucnu.
SOUTĚŽE	
K1	Student je schopen rozlišit různé kybernetické útoky, částečně ovládá právní předpisy týkající se ochrany před těmito útoky a je schopen aplikovat základní preventivní opatření.

Obsah modulu (program přednášek a dalších aktivit)	**Odkaz na výsledky učení**
PŘEDNÁŠKY 1. Sociální inženýrství 2. Spam, podvod, podvod 3. Botnet 4. Kybernetické útoky - Hacking, cracking, malware, ransomware 5. Kybernetické útoky - útoky finanční povahy (phishingpharming, spearphishing, mobilní phishing). 6. Kybernetické útoky - sociální útoky (kyberšikana, stalking, sexting, kybergrooming atd.). WORKSHOPY 1. Analýza jednotlivých útoků - modus operandi 2. Testování zabezpečení proti vybraným útokům. 3. Definice možností prevence jednotlivých typů útoků 4. Návrh řešení na míru pro ochranu před jednotlivými kybernetickými útoky. 5. testování bezpečnosti některých systémů, aplikací a dat. Studenti se pokusí navrhnout vlastní řešení pro zvýšení bezpečnosti těchto systémů, aplikací nebo dat. 6. Seznámení s nástroji a prostředky pro bezpečné ukládání dat a nastavení bezpečné online komunikace (např. správa a nastavení VPN, PGP, správce hesel atd.).	W1, W2 U1, U2, K1

Zůstatek kreditů ECTS		
Forma pracovního zatížení studentů		Počet hodin
Počet hodin s přímou účastí akademického pracovníka		
1.1	Účast na přednáškách	6
1.2	Účast na seminářích	
1.3	Účast na seminářích	14
1.4	Účast na laboratorních činnostech	
1.5	Účast na projektech	
1.6	Účast na konzultacích (2-3krát za semestr)	
1.7	Účast na konzultacích k projektu	
1.8	Účast na zkouškách/testech	2
1.9	Ostatní ...	
1.10	**Počet hodin strávených za přímé asistence akademických pracovníků (součet 1.1 - 1.9)**	22
1.11	**Počet ECTS kreditů, které student získal v předmětech vyžadujících přímou účast akademického pracovníka)**	1
Individuální práce studentů		
2.1	Individuální studium (včetně e-learningových přednášek)	25
2.2	Individuální příprava na semináře	10
2.3	Individuální příprava na test	
2.4	Individuální příprava na laboratorní výuku	
2.5	Příprava zpráv	
2.6	Realizace samostatně prováděných úkolů (projekty, dokumentace)	
2.7	Příprava na závěrečnou zkoušku/testy semináře	5
2.8	Příprava na závěrečnou zkoušku/testování přednášek	5
2.9	Další	
2.10	**Počet hodin individuální práce (součet 2.1 - 2.9)**	45
2.11	**Počet kreditů ECTS získaných studentem v rámci jednotlivých vzdělávacích aktivit**	1,5
Celková pracovní zátěž (h)		**67**
ECTS kredity za modul		**2,5**

Metody ověřování výsledků učení									
Výsledek učení	**Formy kreditních tříd**								
	Ústní zkouška	Písemná zkouška	Částečný písemný úkol	Závěrečný písemný úkol (esej atd.)	Test	Design/prezentace	Nahlásit	Činnosti ve třídě	Ostatní ...
NOVINKY									
W1, W 2		x	x		x			x	
DOVEDNOSTI									
U1						x		x	
U2						x		x	
SOUTĚŽE									
K1						x		x	

Kritéria pro hodnocení kompetencí studentů
Minimální požadavky na tři skupiny výsledků učení, kterých musí student dosáhnout, aby předmět absolvoval, jsou uvedeny níže v syntetické podobě. Aby Student modul absolvoval, musí být všechny výsledky učení popsané v sylabu pozitivně ověřeny osobou (osobami), která (které) modul vyučuje (vyučují).

W - VĚDOMOSTI
Hodnocení:
Uspokojivý - Student si pamatuje a reprodukuje znalosti, které má v rámci modulu zvládnout.
Dobrý - Žák dodatečně interpretuje jevy / problémy a je schopen vyřešit typický problém.
Velmi dobře -Student je schopen řešit i složité problémy v daném oboru, je schopen syntetizovat, provést komplexní hodnocení, vytvořit práci, která je originální a inspirativní pro ostatní.

U - DOVEDNOSTI
Hodnocení:
uspokojivý - student zná podstatu činností a je schopen pod vedením akademického učitele provádět činnosti/řešit problémy související s obsahem modulu.
Dobrý - Student je schopen samostatně provádět činnosti / úkoly / řešit typické problémy související s obsahem modulu.
Velmi dobře - Student si plně osvojil schopnost / dovednost provádět činnosti / úkoly / problémy stanovené v obsahu modulu, a to i ve složitějších případech.

K - SOCIÁLNÍ KOMPETENCE
Hodnocení:
uspokojivě - student pasivně vstřebává obsah modulu, prokazuje schopnost soustředit se a naslouchat.
Dobrý - Žák se aktivně účastní výuky, vytváří hodnotové soudy podle kritérií přijatých v daném oboru, dokáže aktivně spolupracovat ve skupině.
Velmi dobře - Žák integruje postoje podle navrženého modelu, rozvíjí vlastní systém profesních a společenských hodnot, je schopen převzít odpovědnost za jednání skupiny, včetně vedení.

2. Základní materiály pro učitele

Definice (slovníček pojmů)

Kyberkriminalita - nejčastěji se používá pro označení trestných činů spáchaných pomocí informačních technologií a používání tohoto termínu se z normativní oblasti přesunulo i do odborného slovníku.
Kyberkriminalita - je trestný čin, při kterém jsou prostředky informačních a komunikačních technologií **použity jako nástroj ke spáchání trestného činu a jako cíl útoku pachatele,** přičemž **uvedený útok je trestným činem za předpokladu, že jsou tyto prostředky použity nebo zneužity v informačním, systémovém, programovém nebo komunikačním prostředí (tj. kyberprostoru).**
Kyberkriminalitu lze definovat jako jednání namířené proti počítači nebo v některých případech proti počítačové síti nebo jako jednání, při němž je počítač použit jako nástroj ke spáchání trestného činu. Nezbytným kritériem pro použití definice kyberkriminality je, že prostředím, v němž se činnost odehrává, je pak počítačová síť, tj. kyberprostor.
Kybernetická kriminalita - jakýkoli trestný čin, při kterém pachatel využil informační a komunikační technologie.

FP TERMINÁL - Platební podvody. Skupina zaměřená na poskytování podpory v oblasti online podvodů.

FP Cyborg - High-Tech Crimes. Skupina zabývající se různými kybernetickými útoky, které mají dopad na kritickou infrastrukturu a informační systémy, a poskytující jim podporu. Jedná se zejména o útoky typu malware, ransomware, hacking, phishing, krádeže identity atd.

FP Twins - Sexuální zneužívání dětí. Skupina, která se zabývá a poskytuje podporu při vyšetřování sexuálního zneužívání dětí.

Počítačový bezpečnostní incident (který lze chápat jako počítačový útok nebo počítačový zločin) - nezákonná, neoprávněná, nepřijatelná akce, která ovlivňuje počítačový systém nebo síť.
Kybernetický útok[10] - lze tedy definovat jako **jakékoli protiprávní jednání útočníka v kyberprostoru, které je namířeno proti zájmům jiné osoby**.
Kybernetický bezpečnostní incident - je událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb či bezpečnosti a integrity sítí elektronických komunikací.
Kybernetický bezpečnostní incident - je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti poskytování služeb nebo narušení bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetického incidentu.
Počítačová data - jakékoli vyjádření skutečností, informací nebo pojmů ve formě vhodné pro zpracování v počítačovém systému, včetně programu, který je schopen přimět počítačový systém k provedení určité funkce.
Informace - jsou data, která byla zpracována do podoby užitečné pro příjemce. Jakákoli informace je tedy informací, ale jakákoli uložená data se nemusí nutně stát informací.
Sociální inženýrství - zahrnuje ovlivňování, přesvědčování nebo manipulaci lidí s cílem přimět je k určitému jednání nebo od nich získat informace, které by jinak neposkytli.
Botnet lze nejjednodušeji definovat jako síť softwarově propojených botů[11] , kteří provádějí určitou akci na základě příkazu "vlastníka" (nebo správce) této sítě. Takto vytvořená síť může být použita k legitimním činnostem (např. distribuované výpočty) nebo k nezákonným činnostem.
Decentralizovaná architektura - je obvykle postavena na architektuře peer-to-peer (P2P). Tato architektura umožňuje sdílení zdrojů a příkazů v rámci sítě P2P.
Malware - slouží jako prostředek pro přístup, ovládání a další šíření malwaru nebo jiných úkolů podle pokynů útočníka, a to nejen v případě botnetů. Pokud však malware v současné době infikuje počítačový systém uživatele, existuje vysoká pravděpodobnost, že se stal součástí botnetu
Malware - (odvozeno od *škodlivého softwaru)* může být jakýkoli program používaný k narušení standardního provozu počítačového systému, k získání informací (dat) nebo k získání přístupu do počítačového systému. Malware může mít mnoho podob, přičemž mnoho typů malwaru je pojmenováno podle činnosti, kterou provádí.
Adware je zkratka pro "*software podporovaný reklamou".* Jedná se o nejméně nebezpečnou, ale výnosnou formu malwaru.[12]
Spyware vznikl spojením anglických slov "*spy*" a "*software"*. Spyware se používá k získávání statistických údajů[13] o provozu počítačového systému a jejich odesílání do datové schránky útočníka bez vědomí nebo souhlasu uživatele. Tato data mohou zahrnovat i informace osobní povahy nebo informace o osobě uživatele, stejně jako informace o navštívených webových stránkách, spuštěných aplikacích atd.
Viry - jsou programy nebo škodlivé kódy, které se připojují k jinému existujícímu spustitelnému souboru

[10] Je třeba odlišit pojem kybernetický útok od pojmu **bezpečnostní incident, který** představuje porušení bezpečnosti IS/IT a pravidel stanovených k její ochraně (bezpečnostní politika).

[11] **Bot** (zkratka pro robot). Jedná se o program, který může vykonávat příkazy útočníka zadané z jiného počítačového systému. Nejčastějším způsobem je infikování počítače virem, například červem, trojským koněm apod. Počítačový systém, který je takto ovládán na dálku, se pak označuje jako **zombie**. Některé zdroje však infikovaný počítačový systém označují dokonce jako bota.
Bot může shromažďovat data, zpracovávat požadavky, posílat zprávy, komunikovat s řídicím prvkem atd.

[12] Existují společnosti, které se specializují na "pay per install" (*PPI)*. *"PPI" pak vede k množství akcí vedoucích k instalaci doplňků nebo jiného nežádoucího softwaru, který (v nejméně škodlivém případě) uvádí reklamy na webových stránkách bez vědomí uživatele nebo je vkládá tam, kde na webových stránkách žádné reklamy.... **PPI spoléhá na to, že těm, kteří tyto služby nabízejí, je jedno, zda si uživatel chce něco nainstalovat**. **Za každou instalaci dostávají až 1,50 USD,** takže je více než jisté, že podvodné a automatizované instalace jsou podstatnou součástí jejich "obchodního modelu"."*

[13] Např. přehled navštívených webových stránek, jejich IP adresy, přehled nainstalovaných a používaných programů, záznamy o stahování souborů z internetu, údaje o struktuře a obsahu adresářů uložených na pevném disku atd.

(např. softwaru atd.) nebo dokumentu. Virus se replikuje při spuštění tohoto softwaru nebo otevření infikovaného dokumentu. Nejčastěji se viry šíří sdílením softwaru mezi počítačovými systémy; k jejich šíření není nutná spolupráce uživatelů.
Počítačoví červi se také označují jako viry. Důvodem užšího spojení s viry je to, že červi nepotřebují žádného hostitele, tj. nemají spustitelný soubor (jako viry). Na rozdíl od virů, které jsou součástí jiného programu, se tyto programy obvykle šíří samostatně.
Trojské koně jsou obecně takové počítačové programy, které obsahují skryté funkce, s nimiž uživatel nesouhlasí nebo o nichž neví a které jsou potenciálně nebezpečné pro další fungování systému.
Zadní vrátka - některé trojské koně, pokud jsou spuštěny bez vědomí uživatele, otevírají komunikační porty počítače, čímž usnadňují další infikování napadeného systému jiným malwarem nebo usnadňují přímé ovládání infikovaného počítače na dálku.
Skenovací programy[14] ("*skenery portů") - tj.* programy, které slouží především ke zjištění, které porty komunikační sítě počítače jsou otevřené, jaké služby na nich běží a zda je možné na takový systém zaútočit.
Rootkity - označují nejen počítačové programy, ale také všechny technologie používané k maskování přítomnosti škodlivého softwaru (např. počítačových virů nebo trojských koní, červů atd.) v infikovaném systému. Nejčastěji mají podobu nepříliš velkých počítačových programů. Rootkity nejsou samy o sobě škodlivé, ale využívají je tvůrci škodlivých programů, jako jsou viry, spyware atd.[15]
Keylogger - je software, který zaznamenává konkrétní stisky kláves v infikovaném počítačovém systému. Nejčastěji se keylogger používá k záznamu přihlašovacích údajů (uživatelské jméno a heslo) k účtům, ke kterým se přistupuje z počítačového systému. Získané informace jsou pak obvykle odeslány útočníkovi.
Ransomware - je malware, který brání uživatelům v řádném používání počítačového systému nebo je omezuje, dokud útočník neobdrží "výkupné". Ransomware se do počítače nejčastěji dostane prostřednictvím škodlivého softwaru (trojského koně nebo červa), který se nachází na webových stránkách nebo je přílohou e-mailu. Jakmile se malware bezpečně "usadí" v počítačovém systému, stáhne se jeho vlastní ransomware.
Crypto-ransomware - cílem tohoto malwaru je zašifrovat pevný disk nebo vybrané typy souborů v počítačovém systému. Primárně je jeho cílem zašifrovat soukromé soubory uživatele, jako jsou obrázky, textové dokumenty nebo tabulky, videa atd.
Policejní ransomware - poté zablokuje přístup k účtu Windows uživatele[16] a oznámí uživateli, že v jeho počítači byl nalezen materiál porušující zákony dané země (např. porušování autorských práv, dětská pornografie atd.). Současně je uživatel "policií" vyzván, aby zaplatil požadovanou částku, po jejímž zaplacení bude počítač odblokován a celá záležitost "vyřešena".
Spam - lze v zásadě chápat ve dvou rovinách. V **užším slova smyslu se jedná o** hromadné šíření nevyžádaných zpráv, obvykle reklamního charakteru, prostřednictvím internetu a nejčastěji prostřednictvím elektronické komunikace. V **širším slova smyslu** jsou spamem všechny přijaté nevyžádané zprávy, tedy i zprávy obsahující viry, trojské koně apod.[17] .
Spam - je **zpráva zaslaná elektronicky, hromadně a zejména bez žádosti.**
Scam - jako **scam se označuje** spam obsahující kriminální nebo jiný podvodný obsah. Podvody dnes tvoří významnou část spamu a jejich cílem je, obvykle s využitím sociálního inženýrství, získat důvěru uživatele a donutit ho k provedení určitých požadovaných akcí.
Podvod 419 - tak se označují e-maily známé spíše jako **nigerijské dopisy**. Tyto podvody jsou příkladem přenesení běžné trestné činnosti (podvodů) z reálného světa do světa virtuálního.

[14] Tyto programy se někdy označují jako skenovací programy nebo skenery.

[15]Podrobněji viz BALIGA, Arati, Liviu IFTODE a Xiaoxin CHEN. Automatizované omezování útoků rootkitů. *Computers & Security*, 2008, roč. 27, č. 7-8, s. 323-334.

[16] Aplikace byla nastavena na "StayOnTop". Uživatel nevidí ostatní aplikace skryté pod tímto "dialogem ransomwaru" a nemůže vyvolat správce úloh. Samotný Ransomware byl zaregistrován v registrech Run a RunOnce a prováděl kontrolu každých 500 ms a ve stejném časovém rozmezí skryl správce úloh. Jediná další spuštěná aplikace komunikovala se serverem C&C (maskovaná v procesu prohlížeče).

[17] Ke klasifikaci spamu srov. například GONZÁLES-TALAVÁN, Guillermo. Jednoduchý konfigurovatelný filtr spamu SMTP: Greylists. *Computers& Security*, 2006, roč. 25, č. 3, s. 229-236.

Hoax(výmysl, vtip, novinářská faleš) - je další formou spamu nebo hoaxu. Označení "hoax" se používá pro řetězové zprávy (jako např: "*pošli to dál*", "*pokud to nepošleš dalším 20 lidem..... stane se...*" atd.), které obsahují zkreslené, nepravdivé, zavádějící nebo jiné nepravdivé informace. Hoax často obsahuje varování před útokem, popisy hrozeb, prosby o pomoc, výzvy, petice, prohlášení známých osobností, řetězové dopisy pro štěstí, vtipné zprávy, obrázky a videa v prezentacích, hrající si na kočky a jiná zvířata atd.
Podvodné nabídky - jedná se o velmi účinnou formu podvodu. Podvodné nabídky mohou být zasílány hromadně nebo cíleně. V současné době jsou takové nabídky zasílány nejen prostřednictvím e-mailu, ale také prostřednictvím všech druhů rychlých zpráv, sociálních sítí, aukčních webů atd.
Phishing - nejčastěji se definuje jako podvodné nebo klamavé jednání s cílem získat informace o uživateli, jako je uživatelské jméno, heslo, číslo kreditní karty, PIN atd.
Phishing - v **užším slova smyslu je phishing** akce, která vyžaduje, aby uživatel navštívil podvodnou stránku (zobrazující např. stránky internetového bankovnictví, internetového obchodu apod.) a poté vyplnil "přihlašovací údaje" nebo jsou tyto údaje přímo vyžadovány (např. při vyplňování formuláře apod.). **Phishing - v širším slova smyslu** lze phishing definovat jako jakékoli podvodné jednání, jehož cílem je vzbudit v uživateli důvěru, snížit jeho ostražitost nebo ho jinak donutit přijmout scénář předem připravený útočníkem.
Pharming[18] - je sofistikovanější a nebezpečnější forma phishingu. Jedná se o útok na server DNS (Domain Name System), který převádí doménové jméno na IP adresu. K útoku dochází, když uživatel zadá do webového prohlížeče adresu webového serveru, ke kterému chce získat přístup.
Spearphishing - je jednou z forem phishingového útoku, ale rozdíl je v tom, že spearphishing je přesně cílený útok, na rozdíl od phishingu, který je poměrně běžným (náhodným) útokem. Cílem útoku - je obvykle konkrétní skupina, organizace nebo jednotlivec a konkrétně informace a data obsažená v této organizaci (např. duševní vlastnictví, osobní a finanční údaje, obchodní strategie, utajované informace atd.).
Vishing[19] - označuje telefonický phishing, při kterém útočník používá techniku sociálního inženýrství a snaží se od uživatele získat citlivé informace (např. čísla účtů, přihlašovací údaje - jméno a heslo, čísla platebních karet atd.). Útočník se záměrně snaží zfalšovat identitu uživatele. Útočníci se často vydávají za zástupce skutečných bank nebo jiných institucí, aby v uživateli vzbudili co nejmenší podezření. Vishing se používá v telefonii VoIP (Voice over Internet Protocol).
Smishing[20] - funguje na podobném principu jako vishing nebo phishing, ale k šíření zpráv využívá SMS zprávy. Smishing je v podstatě snaha přimět uživatele k zaplacení určité částky (např. zavolání na bezplatnou linku, odeslání SMS dárci apod.) nebo kliknutí na podezřelé odkazy URL. Pokud uživatel takovou adresu URL navštíví, je přesměrován na stránku, která zneužívá určité zranitelnosti počítačového systému, nebo je uživatel vyzván k poskytnutí citlivých informací či malwaru.[21]
Kompromitace firemního e-mailu[22] - jedná se o typ podvodného útoku, při kterém se útočník vydává za vedoucího pracovníka (obvykle generálního ředitele) a snaží se přimět zaměstnance, zákazníka nebo dodavatele, aby mu předali peníze nebo citlivé informace.
CEO FRAUD (forma podvodu BEC) - Útočníci se vydávají za generálního ředitele společnosti nebo jiného vedoucího pracovníka společnosti a posílají zaměstnancům podvržený e-mail s možností zasílat bankovní převody a dávají jim pokyn, aby útočníkům poslali finanční prostředky.
INVOICE (forma podvodu BEC) - společnost, která má často dlouhodobý vztah s dodavatelem, je požádána o převod finančních prostředků na úhradu faktury na jiný, falešný účet. Útočník obvykle kontaktuje oběť prostřednictvím e-mailu nebo telefonu. Útok prostřednictvím e-mailu má obvykle vytvořený zdrojový kód (hlavičku) a předmět žádosti, takže se jeví jako velmi podobný legitimní žádosti.

[18] Jedná se o spojení slov farmingi **phreaking**.
[19] Jedná se o kombinaci slov "voice" a "phishing".
[20] Jedná se o kombinaci slov "SMS" a "phishing".
[21] Např. Xshqi- *Android Worm na čínského Valentýna.* [online]. [citováno 14.8.2016]. Dostupné z: https://securelist.com/blog/virus-watch/65459/android-worm-on-chinese-valentines-day/
Selfmite- *Červ SMS pro Android Selfmite je zpět a je agresivnější než kdy dříve.* [online]. [citováno 14.8.2016]. Dostupné z: http://www.pcworld.com/article/2824672/android-sms-worm-selfmite-returns-more-aggressive-than-ever.html
[22]Podvody BEC jsou známé také jako "CEO fraud" nebo "Man-in-the-Email".

PODVOD ÚČTU (forma podvodu BEC) - tento útok je podobný útoku Falešná faktura. Útočník použije e-mailový účet zaměstnance (hacknutý nebo podvržený) a následně odešle e-mail zákazníkům, ve kterém je informuje, že došlo k problému s jejich platbou a je třeba ji znovu zaslat na jiný účet.
Vydávání se za manažery a právníky (forma podvodu BEC) - oběti jsou kontaktovány útočníky, kteří se vydávají za právníky nebo zástupce právnických firem. Útočník žádá o převod velkého množství finančních prostředků, které mají pomoci vyřešit právní spor nebo zaplatit nezaplacený účet. Útočník se snaží oběti přesvědčit, že převod je důvěrný a časově náročný, takže je méně pravděpodobné, že se zaměstnanec pokusí potvrdit, zda má finanční prostředky převést.
Krádež dat (forma podvodu BEC) - typ podvodu BEC, jehož cílem není přímý převod peněz. Typickými oběťmi tohoto útoku jsou finanční nebo personální oddělení / zaměstnanci. Útočník je požádá o zaslání velmi citlivých údajů na jejich účet. Používá se sociální inženýrství a útok na krádež dat může být výchozím bodem pro výše uvedené útoky BEC zaměřené na finanční převody.
Podvodné webové stránky (společnosti) - Na internetu najdete mnoho aktivit nebo webových stránek[23] , které prezentují úžasné ceny nebo nabízejí různé zboží za velmi přijatelné ceny. Útočníci využívají sociální inženýrství a spoléhají především na nedůvěru a neopatrnost lidí. Vlastní aktivity útočníka pak mohou mít obvykle dvě podoby.
Hacking - je dnes veřejností vnímán pejorativně jako jakákoli činnost osoby, která chce získat nelegální přístup do cizího systému nebo osobního počítače.[24]
Bílé klobouky - White hats: jedná se o hackery, kteří pronikají do systému využíváním zranitelností v zabezpečení systému právě za účelem odhalení těchto zranitelností a vytvoření takových mechanismů a bariér, které by měly takovým útokům zabránit. Často se jedná o zaměstnance nebo externí spolupracovníky renomovaných společností působících v oblasti informačních technologií. Jejich průnik do systému nezpůsobuje uživatelům škody ani jiné újmy, naopak v mnoha případech upozorňují správce takto napadeného systému na bezpečnostní slabiny. Jejich činnost nemá v podstatě destruktivní charakter.
Black hats - Černé klobouky: v podstatě opak hackerů s bílými klobouky. Jejich motivací je snaha způsobit uživateli infikovaného systému škodu nebo jinou újmu, případně získat majetkový či jiný prospěch. Kromě toho, že skutečně dosáhnou prolomení napadeného systému, je v jejich jednání patrný další kriminální prvek.
Grey hats - **Šedé klobouky:** jedná se o šedou zónu hackerů, tedy o lidi, kteří se neprofilovali směrem k těmto dvěma skupinám. Příležitostně mohou porušovat některá práva druhých nebo morální zásady, ale jejich jednání není primárně diktováno snahou škodit, jako je tomu u černých klobouků.
Termín **cracking** - je spojován s termínem hacking, někdy jsou dokonce tyto termíny veřejností nebo v médiích zaměňovány. Z hlediska obsahu znamená pojem cracking prolomení nebo obejití ochranných prvků počítačového systému, programů nebo aplikací s úmyslem jejich následného neoprávněného použití.
Prolamování hesel - je jedna z forem prolamování, která slouží ke zjištění hesla pro přístup do počítačového systému, licencovaného systému nebo programu. Pokud jde o crackování autorských práv, cracker obvykle vytvoří keygen nebo crack[25] , který umožňuje následné používání programu. Takto upravené programy jsou obvykle k dispozici na warezových fórech nebo v sítích P2P.
Internetové pirátství - je obecný pojem zahrnující trestné činy porušující práva duševního vlastnictví (velmi často omezené na autorská práva). Teprve s rozšířením počítačových systémů a zejména s nástupem internetu můžeme hovořit o masovém pirátství jako o jedné z nejrozšířenějších forem počítačové kriminality.
Právo duševního vlastnictví - je nehmotný statek, tzv. hmotný statek, který je **výsledkem tvůrčí činnosti člověka**. Toto právo je **nezávislé na hmotném substrátu** (může být tedy použito kdykoli a kdekoli na světě)

[23] Nejčastěji se jedná o webové stránky, reklamní portály, ale mohou to být i účty na sociálních sítích apod.

[24] Podrobněji viz např. GRIFFITHS, Mark. Počítačová kriminalita a hackerství: vážný problém pro policii? *The Police Journal,* 2000, roč. 73, č. 1, s. 18-24.
YAR, Majid. Počítačové hackerství: jen další případ kriminality mladistvých? *The Howard Journal,* 2005, roč. 44, č. 4, s. 387-399.

[25] **Keygen -** generátor **klíčů.** Program, který generuje sériová čísla nebo jiná data. **Crack** - Program sloužící k odstranění nebo omezení funkčnosti ochranných prvků jiného programu.

za předpokladu, že je **jedinečné, neopakovatelné a dostatečně originální**.
Autorské právo - chrání např. původní literární a umělecká díla, hudební skladby, televizní vysílání, počítačové programy, databáze, reklamní výtvory, multimédia atd.
Průmyslová práva - chrání např. patenty na vynálezy, průmyslové vzory, průmyslové modely, ochranné známky, zeměpisný původ atd.
Softwarové pirátství - porušování autorských práv v souvislosti s počítačovými programy.
Audiovizuální pirátství - porušování autorských práv k audiovizuálním dílům - hudbě a filmu.
Šíření díla e-mailem (případ porušení autorských práv v kyberprostoru) - je nejjednodušší způsob šíření malých souborů (zejména literárních nebo grafických děl chráněných autorským právem).
Zásah do počítačových programů (případ porušení autorských práv v kyberprostoru) - znemožnění pořízení kopií takto chráněných programů technickými prostředky vlastníka autorských práv (tzv. crack).
Šíření díla pomocí dat (případ porušení autorských práv v kyberprostoru) - média přímo mezi uživateli (půjčování a následné kopírování dat z DVD, HDD atd., prodej médií a další).
Nahrávání přímo během promítání a následné šíření záznamu (např. nahrávání filmového díla přímo z plátna) případ porušení autorských práv v kyberprostoru) -camcording.
Neoprávněné předvádění audiovizuálních děl (případ porušení autorských práv v kyberprostoru) - skutečné pořízení počítačového díla. Počítačový program je zvláště chráněn a podle autorského zákona není možné pořizovat rozmnoženiny takového díla, a to ani pro osobní potřebu, bez souhlasu vlastníků autorských práv.
Používání počítačového programu v rozporu s licencí.
Umístění díla (audiovizuálního nebo softwarového) v kyberprostoru (**upload)** představuje šíření díla ve smyslu autorského zákona a (pokud k tomu autor nebo jiná oprávněná osoba nedá svolení) může být trestné. **Neoprávněným užitím díla je rovněž zveřejnění odkazu na místo v kyberprostoru, odkud lze dílo získat.**
Warez - je zjednodušeně řečeno **forma softwarového pirátství, kdy** informační technologie slouží pouze jako prostředek k urychlení šíření nelegálních kopií děl chráněných autorskými právy prostřednictvím internetu. Warezová fóra se v současné době využívají především ke stahování cracků a keygenů, ale i kompletně upravených programů, filmů a hudby.
Sniffing - je metoda nelegálního zachycení dat procházejících počítačovou sítí během komunikace mezi poskytovanou službou a počítačovým systémem pomocí **snifferu.**[26]
DoS - zkratka pro ***odepření služby***. Jedná se o jednu z forem útoku na (internetovou) službu, jejímž cílem je vyřadit z provozu nebo snížit výkonnost napadeného technického zařízení.[27] Tento útok je realizován zahlcením napadeného počítačového systému (nebo síťového prvku) opakovanými požadavky na provedení akce počítačového systému. Tento útok lze realizovat také zahlcením informačních kanálů mezi serverem a počítačem uživatele nebo zahlcením volných systémových prostředků.
Distribuované odepření služby (DDoS) - cílový počítačový systém je přetížen **odesíláním paketů z více počítačových systémů na různých místech, což ztěžuje obranu a identifikaci útočníka**. Tento typ útoku byl použit například proti společnosti Yahoo! Inc, elektronickému obchodu apod.[28]
DRDoS (Distributed Reflected Denial of Service) je podvržený distribuovaný útok DoS, který využívá tzv. mechanismus odrazu. Útok spočívá v zasílání podvržených požadavků na připojení velkému počtu

[26]Sniffing **je** anglický výraz pro slídění nebo špehování. Sniffer je tedy někdo, kdo slídí nebo špehuje.

[27] Podrobněji např. MARCIÁ-FERNANDÉZ, Gabriel, Jesús E. DÍAZ-VERDEJO a Pedro GARCÍA-TEODORO. Vyhodnocení útoku DoS s nízkou rychlostí proti aplikačním serverům. *Computers & Security*, 2008, roč. 27, č. 7-8, s. 335-354.
CARL, Glenn, Richard BROOKS a Rai SURESH. Wavelet-Based Denial-of-Service Detection. *Computers & Security*, 2006, roč. 25, č. 8, s. 600-615.
RAK, Roman a Radek KUMMER. Informačníhrozby v letech 2007-2017. *security magazín,* 2007, roč. 14, č. 1, s. 3.

[28] Například útoky DoS na webové stránky předsednictví, parlamentu, ministerstev, médií a dvou estonských bank - Estonsko (2007). *Estonsko se vzpamatovává z masivního DDoS útoku.* [online]. [cit. 4. 3.2010] Dostupné na: http://www.usatoday.com/tech/news/techpolicy/2007-09-12-spammer-va_N.htmhttp://www.computerworld.com/s/article/9019725/Estonia_recovers_from_massive_DDoS_attack

počítačových systémů, které pak na tyto požadavky odpovídají, ale nikoli iniciátorovi připojení, ale oběti. Je to proto, že *podvržené požadavky na připojení* mají jako zdrojovou adresu adresu oběti, která je pak zaplavena odpověďmi na tyto požadavky.

Ping-Flood - díky protokolu Internet Control Message Protocol a nástroji Ping (Packet Internet Groper) je možné pomocí příkazu "ping" zjistit "životnost" počítačového systému s danou IP adresou a zjistit dobu odezvy takového systému. Při útoku Ping-Flood je oběť zaplavena velkým množstvím tzv. paketů ICMP echo request, na které oběť začne odpovídat - posílá tzv. pakety ICMP Echo Reply.

Zaplavení volných systémových prostředků (*SYN-Flood)* - jedná se o typ útoku, při kterém se útočník snaží zahltit oběť velkým počtem požadavků na připojení. Útočník odesílá cílovému počítačovému systému (oběti) sekvenci příkazových paketů SYN (SYN packets), přičemž cílový systém na každý paket SYN reaguje odesláním paketu SYN-ACK, ale útočník již neodpovídá. Cílový počítačový systém čeká na závěrečné potvrzení, tzv. paket ACK, od iniciátora spojení (útočníka) a má pro toto spojení přiděleny prostředky, jejichž počet je však omezen.

Podvržení **zdrojové adresy** (*IP spoofing)* - jedná se o podvržení zdrojové adresy odesílaných paketů, kdy útočník iniciující spojení ze stroje A s IP adresou **a.b.c.d** vloží jako zdrojovou adresu např. IP adresu d.**c.b.a** a odešle ji na cíl B. Cíl B pak odpoví na tuto zdrojovou adresu, tj. odpověď nesměřuje na IP adresu a.b.c.d, ale na IP adresu **d.c.b.a.**

Útok Smurf - provádí se chybným nastavením systému tak, aby odesílal pakety všem počítačům připojeným k počítačové síti prostřednictvím vysílací adresy.

Šíření zakázaných typů pornografie - jedná se především o šíření pornografického materiálu zobrazujícího kontakt se zvířaty a šíření (nebo držení) "dětské pornografie" (materiál zobrazující nebo jinak zneužívající dítě - osobu mladší 18 let nebo osobu, která vypadá jako dítě).

Šíření nenávistného a extremistického obsahu - trestný čin zahrnuje zejména podporu a propagaci hnutí, které zjevně směřuje k potlačení práv a svobod člověka, vyjadřování sympatií k takovému hnutí, hlásání rasové, etnické a národnostní, náboženské nebo třídní zášti nebo zášti vůči jiné skupině.

Šikana - v reálném světě zahrnuje snahu útočníka ublížit, ponížit, zesměšnit nebo urazit jinou osobu, ať už fyzicky nebo psychicky.

Kyberšikana - pak přesouvá "klasickou šikanu" do virtuálního světa a umožňuje útočníkovi používat nástroje a prostředky, které mohou mít na oběť mnohem větší dopad než v reálném světě.

Kybergrooming - je akt psychologické manipulace s osobou (obvykle pomocí sociálního inženýrství), prováděný prostřednictvím internetu nebo informačních a komunikačních technologií (např. mobilních telefonů atd.). Cílem kybergroomingu je vyvolat v oběti falešnou důvěru a přimět ji tak k osobnímu setkání. Výsledkem takového setkání může být jakýkoli fyzický, sexuální nebo jiný útok na oběť. Obětí kybergroomingu se mohou stát děti i dospělí. Podle statistik jsou nejčastějšími oběťmi dívky ve věku 13-17 let.

Sexting - je jednou z forem nebezpečného chování, zejména v prostředí sociálních sítí, tzv. sexting. Termín sexting vznikl spojením slov sex a textová zpráva, z čehož je zřejmý jeho význam. Jedná se o elektronické šíření textových zpráv, fotografií nebo videí se sexuálním obsahem. Takový sexuálně explicitní materiál může být na sociálních sítích nebo jiných úložištích dat zveřejněn přímo samotnými autory nebo jiným uživatelem, který k takovému materiálu získal přístup. Nejčastěji se tak děje dobrovolným nahráním souborů se sexuálním obsahem, které si odesílatelé sami stáhnou.

Kyberstalking je složenina slov kybernetický a stalking. Původně slovo stalking používali lovci při lovu zvěře a znamenalo sledování zvěře, dokud nebyla zabita.

Kyberstalking je opakované kontaktování oběti, např. prostřednictvím textových zpráv, e-mailů, telefonátů, VoIP, instant messagingu atd. Jednání útočníka se obvykle stupňuje a obvykle vyvolává obavy o soukromí, zdraví nebo život oběti.

Kyberstalker se vyznačuje vytrvalostí a systematičností a není neobvyklé, že si vytvoří několik falešných identit, pod kterými oběť kontaktuje. Kyberstalker může také demonstrovat svou moc a sílu, například

Krádež identity - je útok, při kterém je odcizena virtuální identita[29] , nebo se jedná o převzetí kontroly (trvalé či dočasné) nad touto identitou. Motivem útočníka může být finanční zisk, ale i další výhody související s tím, že útočník jedná jménem jiné osoby, např. přístup k informacím o jiných osobách, přístup k firemním datům apod.
APT - zkratka pro pokročilé a přetrvávající hrozby.
APT - je trvalý, systematický kybernetický útok zaměřený na cílový počítačový systém nebo informační a komunikační technologie cílové organizace. K takovému útoku se používají různé techniky a poměrně velké prostředky a obvykle mohou být napadeny sekundární cíle (např. počítačové systémy, např. opakované DoS nebo jiné útoky), aby se odvedla pozornost od primárního cíle (infiltrace společnosti malwarem), na který se následně útočí.
Kyberterorismus - je v podstatě zneužití informačních a komunikačních technologií (včetně internetu) jako prostředku a prostředí k provedení útoku. Stejně jako v případě klasického konvenčního teroristického útoku se jedná o plánovanou činnost, obvykle politicky nebo nábožensky motivovanou, kterou provádějí spíše malé než vojensky organizované struktury. Cílem těchto skupin je především ovlivnit veřejné mínění. Vzhledem k rychlému šíření informačních a komunikačních technologií po celém světě představuje kyberterorismus významnou hrozbu a je teroristickými skupinami stále častěji využíván.[30]
Mediální terorismus - plánované zneužití masmédií a dalších psychologických zbraní k ovlivnění názorů obyvatelstva jako celku nebo cílových skupin.

Klíčové citace z online materiálů:

- Pro pochopení kybernetických útoků a kybernetické kriminality je nutné znát základní terminologii, která s daným oborem přímo souvisí. V této kapitole jsou uvedeny vybrané odborné i právní termíny.
- Nelze najít oblast lidské činnosti, ve které by se přímo či nepřímo nevyužívala výpočetní technika, respektive informační, informační nebo komunikační technologie.
- Lze tvrdit, že v zásadě **nelze najít oblast lidské činnosti, v níž by se přímo či nepřímo nevyužívala výpočetní technika, informační systém nebo informační či komunikační technologie**.
- Rámcové rozhodnutí Rady EU 2002/584/SVV o evropském zatýkacím rozkazu definuje "**počítačovou trestnou činnost"** jako jednání namířené proti počítači nebo jednání, při němž je počítač prostředkem ke spáchání trestného činu. Definice počítačové trestné činnosti vychází rovněž ze znění evropského zatýkacího rozkazu.
- V mezinárodních úmluvách se pojem "**kyberkriminalita"** nejčastěji používá pro označení trestných činů spáchaných prostřednictvím informačních technologií a používání tohoto pojmu se z normativní oblasti přeneslo i do odborného slovníku. Pojem kyberkriminalita je svou povahou podobný pojmům *"násilná trestná činnost", "trestná činnost mladistvých", "hospodářská trestná činnost" atd. Tyto pojmy označují skupiny trestných činů, které mají nějaký společný faktor, jako je způsob provedení, osoba pachatele (alespoň co do typu) atd. v podstatě může jít o velmi různorodou směsici trestných činů, které spojuje společný faktor (počítač, program, data).*[31]
- Při vymezování obsahu pojmu **kyberkriminalita je** důležité si uvědomit, že s rostoucí možností používání prostředků IKT roste i možnost jejich využití (zneužití) ke spáchání trestného činu. Proto v zásadě neexistuje žádná univerzální, všeobecně přijímaná definice, která by plně postihovala rozsah a hloubku tohoto pojmu.

[29] Virtuální identitou se rozumí jakákoli identita nebo avatar, který osoba používá k interakci v kyberprostoru (např. e-mail, účet na sociální síti,hry, různá online tržiště, počítačový systém atd.). Nezáleží na tom, zda je virtuální identita skutečná nebo falešná, tj. zda představuje skutečnou osobu, nebo zda se jedná o zcela uměle vytvořenou identitu bez reálného základu.

[30] JIROVSKÝ, Václav. *Kybernetickákriminalitanejen o hackingu, crackingu, virech a trojskýchkonech bez tajemnic.* Praha: Grada, 2007, s. 129

[31]Smejkal, Vladimír. *Kybernetická kriminalita.* Plzeň: AleščČeněk, 2015, s. 19.

- "Trestná činnost, v níž se nějakým způsobem objevuje počítač jako souhrn hardwaru a softwaru (včetně dat), nebo se mohou objevit jen některé jeho prvky, případně někdy větší počet počítačů buď samostatných, nebo propojených v počítačové síti, a to buď jako objekt zájmu této trestné činnosti (s výjimkou takové trestné činnosti, jejímiž objekty jsou popsaná zařízení považovaná za nemovitý majetek), nebo jako prostředí (objekt), nebo jako nástroj trestné činnosti (viz počítačová kriminalita)."
- ***Počítačová kriminalita / kybernetická kriminalita*** **-** "trestný čin spáchaný pomocí systému zpracování dat nebo počítačové sítě nebo v přímé souvislosti s nimi."
- V nejobecnější rovině lze kyberkriminalitu definovat jako **jednání namířené proti počítači nebo počítačové síti nebo jako jednání, při němž je počítač využíván jako nástroj ke spáchání trestného činu**. Nezbytným kritériem pro uplatnění definice kyberkriminality je pak skutečnost, že počítačová síť, resp. kyberprostor, je prostředím, v němž se tato činnost odehrává.
- Při definování pojmu kyberkriminalita je nejprve nutné **definovat pojem kriminalita obecně**. Pokud jde o využívání informačních systémů, výpočetní techniky nebo komunikačních zařízení, existuje řada činností, které jsou jistě nežádoucí, ale nejsou trestněprávně postižitelné, ačkoli mohou být pro společnost velmi nebezpečné (škodlivé).
- Při vymezení pojmu kriminalita (a toto vymezení může být podáno z několika hledisek - sociologického, forenzního atd.) vycházíme z definice kriminality jako **souhrnu všech jednání, která lze podřadit pod objektivní stránku upravenou trestním zákonem**. Na **základě této definice tedy kriminalita nezahrnuje taková jednání, která nenaplňují žádný objektivní prvek trestného činu, tj. ani přestupek či jiný správní delikt**. Toto vymezení pojmu trestnosti je poměrně přesné a lze jej použít i v oblasti informačních a komunikačních technologií.
- Kyberkriminalita je tedy trestná činnost, která zahrnuje prostředky informačních a komunikačních technologií:
  a) ***použita jako nástroj ke spáchání trestného činu,***
  b) ***jsou cílem pachatele a*** **uvedený *útok* je trestným** činem,
- **Pod pojmem kyberkriminalita se skrývají tři různé kategorie trestných činů:**
  - **trestné činy, u nichž je individuálním objektem charakterizujícím účel přímo ochrana počítačového systému, jeho zařízení a součástí před určitými typy útoků nebo oprávněné zájmy osob na nerušeném používání těchto technických zařízení,**
  - **trestné činy páchané prostřednictvím informačních a komunikačních technologií,**
  - **jiné kvalifikované trestné činy, které nespadají do první ani druhé kategorie, ale které mohou být v daném případě spáchány rovněž za použití informačních technologií a které splňují výše uvedenou definici, protože k jejich odhalení a objasnění lze použít obdobné postupy odhalování jako při vyšetřování trestných činů první a druhé kategorie (např. obdobně zaměřené znalecké posudky).**
- **<u>Klasifikace podle Úmluvy o počítačové kriminalitě a podle Dodatkového protokolu.</u>**

  Úmluva o kyberkriminalitě rozděluje kyberkriminalitu do čtyř kategorií:

  1. **Trestné činy proti důvěrnosti, integritě a dostupnosti dat a počítačových systémů**;
  2. **Počítačová kriminalita**;
  3. **Trestné činy související s obsahem**;
  4. **Trestné činy související s porušováním autorského práva a práv s ním souvisejících**.
- Další protokol pak definuje další kybernetické trestné činy:
  1. **Šíření rasistických a xenofobních materiálů prostřednictvím počítačových systémů***;*

2. **Rasově a xenofobně motivovaná hrozba***;*
3. **Rasisticky a xenofobně motivovaná urážka***;*

4. **Popírání, hrubé zlehčování, schvalování nebo ospravedlňování genocidy nebo zločinů proti lidskosti.**

- **<u>Klasifikace Výboru odborníků pro kyberkriminalitu</u>**

Podle statutu Výboru expertů Rady Evropy pro kyberkriminalitu z roku 2000 lze kyberkriminalitu rozdělit na:

1. **Podle polohy počítače v době spáchání trestného činu:**
   - *cíl útoku;*
   - *prostředek* (nástroj) *útoku.*
2. **V závislosti na povaze činu:**
   - *tradiční protiprávní jednání* (např. padělání apod.).
   - *nové případy narušení* (např. phishing, DDoS atd.).

- **<u>Klasifikace podle eEurope+</u>**

  Dokument rozděluje počítačovou kriminalitu na:

1. **Trestné činy proti soukromí**
   - Nezákonné shromažďování, uchovávání, úprava, zveřejňování a šíření osobních údajů.
2. **Trestné činy související s počítačovým obsahem**
   - Dětská pornografie, rasismus, podněcování k násilí atd.
3. **Hospodářské trestné činy**
   - Neoprávněný přístup, sabotáž, hacking, přenos virů, počítačová špionáž, počítačové padělání a podvod.
4. **Trestné činy proti duševnímu vlastnictví**[32]

- **<u>Klasifikace počítačové kriminality podle kriminologie</u>**

  Porada a Konrád[33] rozdělují kyberkriminalitu do pěti základních skupin.

1. **Neoprávněný zásah do zadávání dat**
   - změna vstupního dokumentu pro počítačové zpracování,
   - vytvoření dokumentu obsahujícího nepravdivé údaje pro následné zpracování počítačem,
2. **Neoprávněné změny uložených dat**
   - manipulace s daty, neoprávněná manipulace s daty a následný návrat k normálu,
3. **Neoprávněné pokyny pro počítačové operace**
   - přímý pokyn k provedení operace nebo instalaci softwaru, který operaci provede automaticky,
4. **Neoprávněné vniknutí do počítačů, počítačového systému a jeho databází.**
   - informační přístup k databázi bez použití informací,
   - neoprávněné použití informací pro osobní potřebu,

[32]Další podrobnosti: JIROVSKÝ, Václav. *Kybernetickákriminalitanejen o hackingu, crackingu, virech a trojskýchkonech bez tajemnic.* Praha: Grada, 2007, s. 92.
[33]Další podrobnosti: Plzeň: AlešČeněk, 2006, s. 272-274.

- pozměňování, ničení nebo nahrazování informací jinými osobami,
- nezákonné "odposlouchávání" a nahrávání provozu elektronických komunikací.

5. Útok na cizí počítač, software a soubory a data v databázích.

- vývoj útočných programů,
- zavedení viru do počítačového softwaru,
- infekce viry nebo jinými programy.

- **<u>Zaměření Europolu na některé druhy kyberkriminality podle míry škodlivosti</u>**

Europol dodržuje Úmluvu o počítačové kriminalitě a řídí se rozdělením trestných činů v ní obsažených. Na podporu boje proti kyberkriminalitě a na pomoc členským státům bylo v rámci Europolu zřízeno Evropské centrum pro boj proti kyberkriminalitě (EC3)[34] . Tento tým jasně vymezil svou působnost v boji proti kyberkriminalitě a určil následující tři oblasti (ohniska - FP), kterými se zabývá:

FP TERMINÁL - Platební podvody. Skupina zaměřená na poskytování podpory v oblasti online podvodů.

FP Cyborg - High-Tech Crimes. Skupina zabývající se různými kybernetickými útoky, které postihují kritickou infrastrukturu[35] a informační systémy, a poskytující jim podporu. Jedná se zejména o útoky typu malware, ransomware, hacking, phishing, krádeže identity apod.

FP Twins - Sexuální zneužívání dětí. Skupina zabývající se a poskytující podporu při vyšetřování sexuálního zneužívání dětí.

---

[34] *Boj proti kyberkriminalitě v digitálním věku.* [online]. [citováno 7.5.2018]. Dostupné z: https://www.europol.europa.eu/ec3.

[35] Pokud jde o vymezení pojmu kritická infrastruktura, je třeba v České republice (v případě kybernetického prostoru) vycházet ze zákona o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Dále jen zákon o **kybernetické bezpečnosti** nebo **ZKB.** Tento zákon v § 2 písm. b) definuje pojem kritická informační infrastruktura a prvek nebo systém kritické infrastruktury.
Definice pojmu "kritická informační infrastruktura" vychází z právních předpisů upravujících oblast krizového řízení. Kritická informační infrastruktura je součástí kritické infrastruktury, která je definována zákonem č. 240/2000 Sb. o krizovém řízení a o změně některých zákonů (zákon o krizovém řízení), ve znění pozdějších předpisů (dále jen zákon o krizovém řízení). Aby mohl být konkrétní informační systém nebo služba a síť elektronických komunikací zařazen mezi kritickou informační infrastrukturu, musí splňovat definiční kritéria pro kritickou infrastrukturu, dále prvek kritické infrastruktury definovaný v zákoně o krizovém řízení a průřezová a odvětvová kritéria definovaná v nařízení vlády č. 432/2010 Sb. o kritériích pro vymezení prvku kritické infrastruktury.
Oddíl VI představuje oborová kritéria pro definici prvku kritické infrastruktury od účinnosti zákona a kybernetické bezpečnosti. "*Komunikační a informační systémy", G: kybernetická bezpečnost.* Zde byla stanovena odvětvová kritéria pro vymezení konkrétního informačního systému, služby nebo sítě elektronických komunikací jako prvku kritické informační infrastruktury.
Tato definice se však vztahuje pouze na oblast kybernetické bezpečnosti. Obecně **lze kritickou infrastrukturu definovat takto**:

1. Kritickou infrastrukturou se rozumí prvek kritické infrastruktury nebo systém prvků kritické infrastruktury, jehož provoz by měl významný dopad na bezpečnost státu, uspokojování základních životních potřeb obyvatelstva, lidské zdraví nebo hospodářství státu.
2. Prvkem kritické infrastruktury se rozumí budova, zařízení, nástroj nebo veřejná infrastruktura určená podle průřezových a odvětvových kritérií, která jsou definována nařízením vlády č. 432/2010 Sb. o kritériích pro určení prvku kritické infrastruktury.
3. Průřezovým kritériem pro určení prvku kritické infrastruktury je hledisko
   (a) oběti s prahovou hodnotou více než 250 úmrtí nebo více než 2 500 osob s následnou hospitalizací delší než 24 hodin,
   (b) hospodářský dopad s prahovou hodnotou hospodářské ztráty v zemi vyšší než 0,5 % hrubého domácího produktu, nebo
   (c) dopad na společnost s prahovou hodnotou významného omezení poskytování základních služeb nebo jiného vážného narušení každodenního života více než 125 000 osob.

- **<u>Klasifikace kyberkriminality podle jejího "vztahu" k digitálnímu prostředí</u>**

  S rozvojem kyberkriminality jako takové se v posledních letech objevil názor, který postuluje možnost nahlížet na kyberkriminalitu jako na čin, který lze označit za "čistou" nebo "pravou" kyberkriminalitu.

  Podle výše uvedeného rozdělení by pak bylo možné chápat kyberkriminalitu jako:

  - Úzké pojetí ("čistá" kyberkriminalita);
  - Široký pojem ("běžné" kriminální chování v novém prostředí).

- **Kybernetický útok**[36] lze definovat jako **jakékoli protiprávní jednání útočníka v kyberprostoru, které je namířeno proti zájmům jiné osoby**. Tato jednání nemusí mít vždy podobu trestného činu.
- Úspěch kybernetického útoku je obvykle založen na narušení jednoho z prvků, které tvoří kybernetickou bezpečnost (**lidé, procesy a technologie)**. **Tyto prvky je třeba uplatňovat nebo upravovat v průběhu celého životního cyklu**. **Týkají se zejména prevence, detekce a reakce na útok.**
- **Kybernetická bezpečnostní událost** je "událost, *která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb nebo bezpečnosti a integrity sítí elektronických komunikací*". Ve skutečnosti se jedná o událost bez reálných negativních důsledků pro daný komunikační nebo informační systém. V podstatě se jedná pouze o hrozbu, která však musí být reálná.
- **Kybernetický bezpečnostní incident** je "*narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti poskytování služeb nebo narušení bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické události*".
- Počítačovými daty se rozumí *"jakékoli vyjádření skutečností, informací nebo pojmů ve formě vhodné pro zpracování v počítačovém systému, včetně programu, který je schopen přimět počítačový systém k provedení určité funkce".*
- Informace *"jsou data, která byla zpracována do podoby, jež je pro příjemce užitečná. Jakákoli informace je tedy informací, ale jakákoli uložená data se nemusí nutně stát informací."*

Úmluva o kyberkriminalitě

- Na prvním místě je třeba zmínit **Úmluvu o kyberkriminalitě a související dodatkový protokol, neboť se jedná o dva nejdůležitější právní dokumenty, které** přispívají k ochraně společnosti před kyberkriminalitou a stanoví základní rámec pro kyberkriminalitu a zároveň poskytují prostředky pro její odhalování a vyšetřování. Dále budou představeny právní dokumenty EU a ES týkající se kyberkriminality
- Úmluvu o kyberkriminalitě schválil Výbor ministrů Rady Evropy na svém 109. zasedání dne 8.th listopadu 2001. Úmluva o kyberkriminalitě byla otevřena k podpisu 23.rd listopadu 2001 v Budapešti.[37] Úmluva vstoupila v platnost 1.st července 2004.
- Úmluva o počítačové kriminalitě[38] se skládá z **preambule** a **48 článků,** které jsou rozděleny do 4 kapitol:

[36] Je třeba odlišit pojem kybernetický útok od pojmu **bezpečnostní incident, který** představuje porušení bezpečnosti IS/IT a pravidel stanovených k její ochraně (bezpečnostní politika).
[37] Seznam zemí, které podepsaly a ratifikovaly Úmluvu o kyberkriminalitě, najdete na adrese: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=F6wSLE5D.
[38] Úplné znění úmluvy najdete na adrese: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

Použité termíny

Opatření, která je třeba přijmout na vnitrostátní úrovni

Část 1 - Trestní právo hmotné (články 2 až 13)

Část 2 - Procesní právo (články 14-21)

Část 3 - Příslušnost (článek 22)

Mezinárodní spolupráce

Část 1 - Obecné zásady (články 23-28)

Část 2 - Zvláštní ustanovení (články 29 až 35)

Závěrečná ustanovení

- Důležitým krokem ke sjednocení práva je vymezení čtyř základních skupin trestných činů (viz kapitola II; články 2-13) a zakotvení dalších obecných ustanovení trestního práva hmotného v nich

Trestné činy proti důvěrnosti, integritě a dostupnosti dat a počítačových systémů. (články 2-6),

Počítačové trestné činy. (články 7-8),

Trestné činy související s obsahem. (článek 9),

Trestné činy související s porušováním autorského práva a práv s ním souvisejících. (článek 10).

- **Dodatkový protokol 189 k Úmluvě o počítačové kriminalitě Rady Evropy**[39] , přijatý dne 28.th ledna 2003.[40] , vymezuje rozsah trestných činů, na které se nevztahuje Úmluva o počítačové kriminalitě. Úmluva o kyberkriminalitě nezahrnuje trestné činy týkající se šíření určitého "*škodlivého materiálu*".[41]

- Dodatkový protokol se skládá z **preambule** a **16 článků,** které jsou rozděleny do 4 kapitol:

1. **Společná ustanovení**
2. **Opatření, která je třeba přijmout na vnitrostátní úrovni**
    - Článek3 – Šíření rasistických a xenofobních materiálů prostřednictvím počítačových systémů
    - Článek 4 - Výhrůžky motivované rasismem a xenofobií
    - Článek 5 - Rasově a xenofobně motivované urážky
    - Článek6-Popírání, hrubé zlehčování, schvalování nebo ospravedlňování genocidy nebo zločinů proti lidskosti
3. **Vztah mezi Úmluvou o kyberkriminalitě a Dodatkovým protokolem**
4. **Závěrečná ustanovení**

- Pokud bychom chtěli definovat pojem sociální inženýrství, mohli bychom říci, že zahrnuje ovlivňování, přesvědčování nebo manipulaci s lidmi s cílem přimět je k určitému jednání nebo od nich získat informace, které by jinak neposkytli.

- V případě sociálního inženýrství je jedním z klíčových faktorů získat co nejvíce informací o cíli útoku (ať už se jedná o počítačový systém, právnickou nebo fyzickou osobu). Často dochází k dlouhodobé

[39] *Dodatkový protokol č. 189 k Úmluvě o počítačové kriminalitě týkající se trestnosti činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů* [online]. [cit. 20.8.2016]. Dostupné z: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168008160f

[40] Seznam zemí, které podepsaly a ratifikovaly dodatkový protokol, najdete na adrese: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189/signatures?p_auth=F6wSLE5D

[41] S výjimkou dětské pornografie, která je přímo zahrnuta v článku 9 Úmluvy o počítačové kriminalitě.

interakci s klíčovou osobou a budování "důvěry" mezi útočníkem a obětí před útokem, přičemž útočník obvykle využívá neopatrnosti lidí, důvěry, touhy pomoci druhým, lenosti, slabosti, strachu (např. z průšvihu), nezodpovědnosti, hlouposti apod.

- Útoky sociálního inženýrství se obvykle provádějí třemi způsoby, které se kombinují:
  1. **Shromažďování volně** (veřejně) **dostupných údajů** o cíli útoku.
  2. **Fyzický útok** (např. útočník se vydává za zaměstnance servisní agentury - např. servisní technik tiskárny, údržbář apod.), při kterém se útočník snaží získat co nejvíce informací "zevnitř" firmy nebo citlivé informace o jednotlivých zaměstnancích (např. prostřednictvím prohledávání odpadkových košů – dumpster diving).
  3. **Psychologický útok**

  Mezi nejčastější metody útoků sociálního inženýrství patří:

  1. **Podvodný e-mail** nebo **falešná webová stránka**
  2. **Telefonní hovor**
  3. **Útok tváří v tvář**
  4. **Potápění v popelnicích** a "napínání dat"
  5. **Vyhledávání na webových stránkách, sociálních sítích atd.** (Jedná se o snadno dostupný, otevřený zdroj dat pro útočníky sociálního inženýrství, který pomáhá identifikovat nebo ověřit informace o potenciálním cíli). **Veřejné informace dostupné online (např.** online publikované životopisy, diplomové práce, články, návrhy atd.) **Výroční zprávy a další veřejně dostupné informace o společnostech.**
  6. **Dodání reklamních nebo jiných materiálů na CD, DVD nebo jiných paměťových médiích.**
  7. **ponechání datového nosiče** (USB apod.) **na zájmovém místě (např. ve** firmě, u zaměstnance doma apod., takový nosič pak obvykle obsahuje malware).
  8. **Nabídka vyzkoušení online služby (např.** nabídka cloudového úložiště nebo zajímavé služby zdarma apod.).
  9. **Dodávka nebo nalezení zařízení (**počítačový systém)
  10. **Falešný servisní technik**
  11. **Další**
- Botnet lze nejjednodušeji definovat jako síť softwarově propojených botů[42] , kteří provádějí určitou akci na základě příkazu "vlastníka" (nebo správce) této sítě. Takto vytvořená síť může být použita k legitimním činnostem (např. distribuované výpočty) nebo k nezákonným činnostem.
- Pro **botnet** je typické, že pokud **je cílový počítačový systém infikován, tento systém,** známý jako "zombie" nebo "bot", **se připojí k centrálnímu řídicímu serveru** [nazývanému příkazový a řídicí server (C&C)]. **Celý systém** (obsahující zombie a C&C) **je ovládán útočníkem** (označovaným jako botmaster nebo botherder), **který ovládá boty prostřednictvím serveru C&C**.[43]

---

[42] **Bot** (zkratka pro robot). Jedná se o program, který může vykonávat příkazy útočníka zadané z jiného počítačového systému. Nejčastějším způsobem je infikování počítače virem, například červem, trojským koněm apod. Počítačový systém, který je takto ovládán na dálku, se pak označuje jako **zombie**. Některé zdroje však infikovaný počítačový systém označují dokonce jako bota.
Bot může shromažďovat data, zpracovávat požadavky, posílat zprávy, komunikovat s řídicím prvkem atd.

[43] Další podrobnosti viz PLOHMANN, Daniel, Elmar GERHARDS-PADILLA a Felix LEDER. *Botnety: detekce, měření, dezinfekce a obrana.* ENISA, 2011 [online]. [cit.17.5.2015], s. 14. Dostupné z: https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence.
Další definice botnetů a informace o nich lze nalézt například na adrese:
Co je to botnet a jak sešíří? [online]. [citováno 15.7.2016]. Dostupné z:
https://www.youtube.com/watch?v=ywXqDon5Xtg

- Pro botnet jsou charakteristické (podstatné) následující prvky:
  1. **Infrastruktura velení a řízení (C&C)**

     Jedná se o infrastrukturu, která se skládá z řídicího prvku (nebo prvků) a botů (řízených počítačovými systémy).

  2. **Instalace a ovládání bota**

     Obvykle se jedná o malware, který se šíří prostřednictvím botnetu nebo jiným způsobem. Hlavním účelem takového malwaru je zapojit do botnetu další počítačové systémy. Malware využívá různé zranitelnosti počítačových systémů.

  3. **Ovládání botů prostřednictvím infrastruktury C&C**

     Bot je software, který pracuje skrytě a ke komunikaci se serverem C&C využívá oblíbené komunikační kanály (IRC, IM, RFC 1459 atd.). Noví boti se snaží získat co nejvíce informací z prostředí a propagovat se v dalších počítačových systémech.

- Na základě architektury lze botnety rozlišit na:

1. **Centralizovaná architektura**

   Tato architektura je obvykle postavena na principu komunikace klient-server. Koncové počítačové systémy (zombie/boty) komunikují přímo se serverem C&C (centrálním řídicím prvkem) a vykonávají instrukce a využívají zdroje z tohoto serveru.

2. **Decentralizovaná architektura**

   Obvykle je postaven na architektuře P2P (peer-to-peer). Tato architektura umožňuje sdílení zdrojů a příkazů v rámci sítě P2P. Ve své "klasické" podobě neobsahuje žádný centrální řídicí prvek, díky čemuž je systém odolnější vůči pokusům o převzetí kontroly prostřednictvím tohoto řídicího prvku

- Botnet je možné kategorizovat jako strukturu **zločinu jako služby** (kdy je nabízena služba: **botnet jako služba)** nebo jako ekonomiku malwaru[44] , kdy poskytuje základní technickou platformu potřebnou k provádění řady kybernetických útoků.

- **Možné trestní sankce v Polsku**

  Nedovolený přístup do systému (hacking) Čl. 267 § 1 a 2 trestního zákoníku. Tento trestný čin je stíhán na žádost poškozeného. Trestá se pokutou, omezením svobody nebo odnětím svobody až na 2 roky.

- **Možné trestní sankce v České republice**
  Pokud jde o vlastní činnost útočníka spočívající v instalaci škodlivého softwaru s cílem následně ovládnout počítačový systém, je možné toto jednání posoudit podle **§ 230** trestního zákoníku (Neoprávněný přístup k počítačovému systému a nosiči informací). Pokud by útočník umístil škodlivý software do počítačového systému s úmyslem způsobit jinému škodu nebo jinou újmu nebo získat pro sebe nebo jinou osobu neoprávněný prospěch, bylo by možné jeho jednání kvalifikovat podle § 230 odst. 2 písm. d) trestního zákoníku.

Botnety: nováinternetováhrozba. [online]. [citováno 15.7.2016]. Dostupné z: http://www.lupa.cz/clanky/botnety-internetova-hrozba/.
Válkysíťovýchrobotů - jak fungujísítěbotnets. [online]. [citováno 15.7.2016]. Dostupné z: http://tmp.testnet-8.net/docs/h9_botnet.pdf.
Botnety. [online]. [citováno 15.7.2016]. Dostupné z: https://www.youtube.com/watch?v=-8FUstzPixU&index=2&list=PLz4vMsOKdWVHb06dLjXS9B9Z-yFbzUWI6.

[44] Správa malwaru. Další podrobnosti naleznete v: PLOHMANN, Daniel, Elmar GERHARDS-PADILLA a Felix LEDER. *Botnety: detekce, měření, dezinfekce a obrana.* ENISA, 2011 [online]. [cit.17.5.2015], s. 21. Dostupné z: https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence.

- **Možné trestní sankce v Portugalsku**
  Podle čl. 6 odst. 2 *zákona o počítačové kriminalitě* je trestné neoprávněným přístupem k jednomu nebo více počítačovým zařízením neoprávněné zavedení jakéhokoli počítačového programu, spustitelné instrukce, kódu nebo dat určených k neoprávněnému spuštění do počítačového systému. Totéž platí pro trestné činy poškození počítačových programů nebo jiných počítačových dat [zásah do dat] (čl. 4 odst. 3), počítačové sabotáže [nezákonný zásah] (čl. 5 odst. 2) a nezákonného odposlechu (čl. 7 odst. 3).
- **Malware** (škodlivý software) může být jakýkoli software používaný k narušení standardního provozu počítačového systému, k získávání informací (dat) nebo k získání přístupu do počítačového systému. Malware může mít mnoho podob a mnoho typů malwaru je pojmenováno podle činností, které vykonávají

    1. **Adware**
    2. **Spyware**
    3. **Viry**
    4. **Červi**
    5. **Trojské koně**
    6. **Zadní vrátka**
    7. **Rootkity**
    8. **Keylogger**
    9. **Ransomware**

- Termín adware je zkratkou pro "*software podporovaný* reklamou". Jedná se o nejméně nebezpečnou, ale výnosnou formu škodlivého softwaru.[45] Adware zobrazuje v počítačovém systému uživatele reklamy (např. vyskakovací okna v operačním systému[46] nebo na webových stránkách, reklamy zobrazované společně se softwarem apod.)
- Spyware vznikl spojením anglických slov "*spy*" a "*software"*. Spyware se používá k získávání statistických údajů[47] o provozu počítačového systému a jejich odesílání do datové schránky útočníka bez vědomí nebo souhlasu uživatele. Tato data mohou zahrnovat i informace osobní povahy nebo informace o osobě uživatele, stejně jako informace o navštívených webových stránkách, spuštěných aplikacích atd.
- Spyware může být nainstalován jako samostatný škodlivý software a často také jako součást jiného, bezplatného a jinak zcela bezpečného softwaru. V takovém případě se instalace a další činnosti spywaru obvykle řeší podle podmínek smlouvy EULA a uživatel obvykle nevědomky dobrovolně souhlasí se sledováním své vlastní činnosti.

---

[45] Existují společnosti, které se specializují na "pay per install" (*PPI*). *"PPI" pak vede k množství akcí vedoucích k instalaci doplňků nebo jiného nežádoucího softwaru, který (v nejméně škodlivém případě) uvádí reklamy na webových stránkách bez vědomí uživatele nebo je vkládá tam, kde na webových stránkách žádné reklamy.... **PPI spoléhá na to, že těm, kteří tyto služby nabízejí, je jedno, zda si uživatel chce něco nainstalovat**. **Za každou instalaci dostávají až 1,50 USD,** takže je více než jisté, že podvodné a automatizované instalace jsou podstatnou součástí jejich "obchodního modelu"."*

[46] Kresba těchto vyskakovacích oken. Další podrobnosti naleznete v části *Adware.* [Online]. [citováno 10.8.2016]. Dostupné z: http://www.mhsaoit.com/computer-networking-previous-assignments/324-lesson-16-h-the-secret-history-of-hacking

[47] Např. přehled navštívených webových stránek, jejich IP adresy, přehled nainstalovaných a používaných programů, záznamy o stahování souborů z internetu, údaje o struktuře a obsahu adresářů uložených na pevném disku atd.

- Spyware představuje hrozbu jednak proto, že odesílá různé informace z počítačového systému uživatele "útočníkovi" (které jsou dále zpracovávány a korelovány s údaji a informacemi získanými z jiných zdrojů
- Existuje velké množství virů, jejichž účelem je destrukce, zatímco jiné jsou navrženy tak, aby se "usadily" v co největším počtu počítačových systémů a poté je využily k cílenému útoku. Pro tyto programy je typická schopnost šířit se mezi systémy bez zásahu uživatele do počítačového systému.
- Podle toho, jaké soubory viry infikují, je lze rozdělit na:
    - bootovací viry (infikují pouze systémové oddíly).
    - souborové viry (infikují pouze soubory)
    - vícesložkové viry (infikují jak soubory, tak oblasti systému).
    - Makroviry (napadají aplikace, které používají makra).
- Takzvaní **počítačoví** červi jsou také označováni jako viry. Důvodem užšího spojení s viry je to, že červi nepotřebují žádného hostitele, tj. nemají spustitelný soubor (jako viry). Na rozdíl od virů, které jsou součástí jiného programu, se tyto programy obvykle šíří samostatně. Poškozený systém pak červ využívá k dalšímu rozesílání svých kopií ostatním uživatelům prostřednictvím síťové komunikace
- **Trojské koně** jsou obecně takové počítačové programy, které obsahují skryté funkce, s nimiž uživatel nesouhlasí nebo o nichž neví a které jsou potenciálně nebezpečné pro další fungování systému. Stejně jako viry mohou být tyto programy přibaleny k jinému bezpečnému programu nebo aplikaci, nebo se mohou tvářit jako neškodný počítačový program. Trojské koně se na rozdíl od klasických virů nedokážou replikovat nebo šířit bez "pomoci" uživatele. Pokud je trojský kůň aktivován, může být použit například ke smazání, zablokování, úpravě, kopírování dat nebo narušení počítačového systému či počítačových sítí.
- Některé trojské koně, pokud jsou spuštěny bez vědomí uživatele, otevírají komunikační porty počítače, což usnadňuje dalším škodlivým programům další infikování napadeného systému nebo usnadňuje přímé ovládání infikovaného počítače tzv. na dálku. Takové trojské koně se označují jako **zadní vrátka**.[48]
- **Rootkity -** tento termín se vztahuje nejen na počítačové programy, ale také na všechny technologie používané k maskování přítomnosti škodlivého softwaru (např. počítačových virů nebo trojských koní, červů atd.) v infikovaném systému. Nejčastěji mají podobu nepříliš rozsáhlých počítačových programů. Rootkity nejsou samy o sobě škodlivé, ale využívají je tvůrci škodlivých programů, jako jsou viry, spyware atd.[49]
- Rootkit mění chování celého operačního systému, jeho částí nebo dalších aplikací tak, aby uživatelé nevěděli o existenci škodlivých programů ve svém počítačovém systému. Obecně lze rootkity rozdělit na **systémové** rootkity (modifikující jádro) a **aplikační rootkity** (modifikující konfiguraci aplikací).[50]
- Keylogger je software, který zaznamenává konkrétní stisky kláves v infikovaném počítačovém systému. Nejčastěji se keylogger používá k záznamu přihlašovacích údajů (uživatelské jméno a heslo) k účtům, ke kterým se přistupuje z počítačového systému. Získané informace jsou pak obvykle odeslány útočníkovi.
- Ransomware bude podrobněji popsán v samostatné kapitole.

[48] Přehled nejběžnějších trojských koní, včetně seznamu jejich funkcí a komunikačních portů, lze získat na různých stránkách dostupných na internetu. Podrobnější informace naleznete např. na adrese http://www.test.bezpecnosti.cz/full.php.

[49] Podrobněji viz BALIGA, Arati, Liviu IFTODE a Xiaoxin CHEN. Automatizované omezování útoků rootkitů. *Computers & Security*, 2008, roč. 27, č. 7-8, s. 323-334.

[50] Srov. RAK, Roman a Radek KUMMER. Informačníhrozby v letech 2007-2017. *security magazín*, 2007, roč. 14, č. 1, s. 5.

Distribuce malwaru

Malware lze do cílového počítačového systému dostat mnoha způsoby.

Několik způsobů šíření malwaru.

Malware se může šířit prostřednictvím:

Přenosná paměťová média

Například pomocí disků CD, DVD, USB, externího disku atd. Jedná se o nejstarší, ale stále účinný způsob šíření malwaru, kdy si uživatelé předávají infikované soubory navzájem nebo v **počítačových sítích, které infikované soubory** obsahují (sdílení takových souborů v rámci počítačových sítí, obvykle sítí P2P).

Stahování z webu

Jedním z nejčastějších způsobů, jak se nakazit škodlivým softwarem, je stažení z internetu a následné spuštění souboru, obvykle s příponou .exe (spustitelný soubor), z neznámého zdroje. Může se jednat o falešné nebo padělané programy (např. napodobeniny Flapp Bird, falešné multimediální kodeky atd.), programy sloužící k obcházení ochrany autorských práv (cracky, keygeny atd.)**, skutečné infikované programy atd.**

- **Škodlivý software lze nainstalovat téměř do každého počítačového systému.** Příkladem specifických instalací je instalace **mikromalwaru.** Jedná se o škodlivý kód, který se šíří v relativně malém počtu počítačových systémů.
- Většina zařízení se systémem Android neumožňuje aktualizaci operačního systému na nejnovější verzi, která je obvykle upravena tak, aby odolávala známým bezpečnostním zranitelnostem a měla již opravené chyby z předchozích verzí tohoto operačního systému. Ve skutečnosti se odhaduje, že 77 % hrozeb napadajících operační systém Android by bylo možné eliminovat použitím nejnovější verze tohoto operačního systemu.
- U mobilních zařízení útočníci používají především:
    - **zastaralá verze operačního systému mobilního zařízení (**známé zranitelnosti jednotlivých systémů);
    - **minimální ochrana mobilního zařízení** pomocí antivirových opatření;
    - **neznalost uživatelů** (mnozí uživatelé z nedbalosti instalují aplikace "z neznámého zdroje" nebo aplikace, které vyžadují nadměrný přístup a oprávnění v rámci zařízení);
    - **sociální inženýrství a "vlny zájmu" o aplikace určitého typu.**
- **Možné trestní sankce v Polsku**
  Porušení integrity dat (viry, trojské koně) - 268 trestního zákoníku, čl. 268a trestního zákoníku. Tento trestný čin se týká mimo jiné krádeže osobních údajů, jejich zpřístupnění třetím osobám bez souhlasu vlastníka a jejich neoprávněného použití. Za spáchání těchto činů jsou stanoveny finanční sankce (až do výše 100 000 PLN).
- **Možné trestní sankce v České republice**
  V České republice může být útok pomocí malwaru trestán podle § **230** (Neoprávněný přístup k počítačovému systému a nosiči informací) trestního zákoníku. Držení malwaru v úmyslu spáchat trestný čin podle § 182 (Porušení tajemství dopravovaných zpráv) nebo trestný čin podle § 230 trestního zákoníku je trestným činem podle § 231 (Získání a přechovávání přístupových hesel k zařízením a počítačovým systémům a jiných podobných údajů) trestního zákoníku. Pokud by cílem viru bylo například získání utajovaných informací nebo podpora teroristické skupiny, mohl by se

útočník **ve fázi přípravy** dopustit například trestných činů podle **§ 311 (Teroristický útok), § 316 (Zpravodajství) nebo § 317 (Ohrožení utajovaných informací) trestního zákoníku**.

- **Možné trestní sankce v Portugalsku**
  Podle čl. 6 odst. 2 *zákona o počítačové kriminalitě je* trestné vytváření, šíření nebo distribuce počítačového programu, spustitelného pokynu, kódu nebo dat určených k provedení nezákonného přístupu do počítačového systému. Totéž platí pro trestné činy poškození počítačových programů nebo jiných počítačových dat [zásah do dat] (čl. 4 odst. 3), počítačové sabotáže [nezákonný zásah] (čl. 5 odst. 2) a nezákonného odposlechu (čl. 7 odst. 3), neboť portugalský zákonodárce nezvolil jediné ustanovení o zneužití zařízení, jak to učinila Budapešťská úmluva (článek 6).

Ransomware

- Do této skupiny malwaru patří také tzv. vyděračský malware, pro který se vžil termín **ransomware**[51] (někdy se označuje také jako rogueware nebo scareware). Ransomware je malware, který brání uživatelům v řádném používání počítačového systému nebo je omezuje, dokud útočník neobdrží "výkupné". Ransomware se do počítače uživatele nejčastěji dostane prostřednictvím škodlivého softwaru (trojského koně nebo červa), který se nachází na webových stránkách nebo je přílohou e-mailu. Jakmile se malware bezpečně "usadí" v počítačovém systému, je stažen jeho vlastní ransomware.
- **Prvním typem je ransomware, který omezuje funkčnost celého počítačového systému** a neumožňuje uživateli systém vůbec používat (např. brání spuštění operačního systému nebo uzamkne obrazovku systému. Typickým příkladem tohoto typu je "*policejní ransomware"* - viz níže).
- **Druhým typem je ransomware, který ponechává počítačový systém funkční, ale uzamkne data uživatele a znemožní k nim přístup.**
- V současné době se používá druhý typ ransomwaru, známý jako **crypto-ransomware**. Cílem tohoto malwaru je zašifrovat pevný disk nebo vybrané typy souborů v počítačovém systému. Primárně je jeho cílem zašifrovat soukromé soubory uživatele, jako jsou obrázky, textové dokumenty nebo tabulky, videa atd.
- Masový výskyt ransomwaru lze datovat přibližně do roku 2011, kdy se po celém světě začal šířit ransomwarový útok blokující přístup k účtu uživatele systému Windows a oznamující, že počítač byl zablokován státní policií.
- V Evropě se postupně objevily různé verze (vzhled stránek) policejního ransomwaru. První verze byla zaznamenána na konci roku 2011, zobrazovala IP adresu připojení, připojení poskytovatele připojení a polohu [kde byla uvedena IP adresa konkrétního poskytovatele připojení (ISP)], pokud měl uživatel zapnutou webovou kameru, byl vytvořen a zobrazen obrázek.
- **Od roku 2013 došlo v oblasti ransomwaru k výraznému posunu. Útočníci omezili útoky spočívající v omezení funkčnosti celého počítačového systému a zaměřili se především na zablokování uživatelských dat.**
- Služba Crime-as-a-service nabízí **ransomware jako službu** od roku 2016**.** Uživatel (tj. útočník) má možnost definovat si vlastní ransomware podle svých představ. Zároveň získává technické zázemí v podobě serverů C&C, bitcoinových peněženek, nepřetržité online podpory atd. Příkladem ransomwaru jako služby je software **Ransom32.**

[51]NapříkladReventon, CryptoLocker, CryptoWall, Loky, Petya, Cerber, SamSam, JigSaw atd. Podrobnější informace naleznete např. v článku:
Ransomware. [online]. [citováno 14.8.2016]. Dostupné z: https://www.trendmicro.com/vinfo/us/security/definition/ransomware.

- **Možné trestní sankce v Polsku**
  V Polsku platí tyto zákony:
  Článek 267 Nezákonné získávání informací
  Článek 269a. Zásah do systému nebo sítě IKT
- **Možné trestní sankce v České republice**
  V České republice může být útok malwarem, jako je ransomware, trestný podle § 230 (Neoprávněný přístup k počítačovému systému a nosiči informací) trestního zákoníku. Držení malwaru s úmyslem spáchat trestný čin podle § 182 (Porušení tajemství dopravovaných zpráv) nebo trestný čin podle § 230 trestního zákoníku je trestným činem podle § 231 (Získání a přechovávání přístupových hesel k zařízením a počítačovým systémům a jiných podobných údajů) trestního zákoníku.
  V případě ransomwaru je možné použít i ustanovení § 230 odst. 3 trestního zákoníku, pokud se útočník dopustí takového trestného činu v úmyslu získat pro sebe nebo jiného neoprávněný prospěch. Rovněž je možné uvažovat o aplikaci ustanovení § 175 (Vydírání) trestního zákoníku, kdy je osoba nucena k zaplacení částky pod pohrůžkou způsobení jiné závažné újmy (např. podáním trestního oznámení[52]]).
- **Možné trestní sankce v Portugalsku**
  Stejně jako téměř ve všech právních řádech nejsou útoky ransomwaru nijak zvlášť trestné, ačkoli takové jednání může být stíháno jako vydírání. Alternativou z hlediska čistě kybernetické kriminality by byl počítačový podvod (článek 221 trestního zákoníku), neboť jeho věcná působnost je poměrně široká a navazuje na znění analogického trestného činu v textu *Budapešťské úmluvy* (článek 8).

Spam

- Z hlediska informačních a komunikačních technologií lze obsah pojmu spam chápat v zásadě ve dvou rovinách. V **užším smyslu** se jedná o hromadné šíření nevyžádaných zpráv, obvykle reklamního charakteru, prostřednictvím internetu, a to nejčastěji prostřednictvím elektronické komunikace. V **širším slova smyslu jsou spamem** všechny přijaté nevyžádané zprávy, a tedy i zprávy obsahující viry, trojské koně apod. [53]
- Charakteristickým znakem spamu je, že se jedná o **zprávu zasílanou elektronicky, hromadně a především bez vyžádání.**
- Podvod 419 je označení pro e-maily, známé spíše jako **nigerijské dopisy**. Tyto podvody jsou příkladem přenesení běžné trestné činnosti (podvodů) z reálného světa do světa virtuálního.
- Další formou spamu nebo mystifikace je hoax (výmysl, vtip, novinářská kachna). Označení "hoax" se používá pro řetězové zprávy (jako např: "*pošli to dál*", "*pokud to nepošleš dalším 20 lidem..... stane se...*" atd.), které obsahují zkreslené, nepravdivé, zavádějící nebo jiné nepravdivé informace. Háček často obsahuje varování před útokem, popisy hrozeb, prosby o pomoc, výzvy, petice, prohlášení známých osobností, řetězové dopisy pro štěstí, vtipné zprávy, obrázky a videa v prezentacích, hrající si kočky a jiná zvířata atd.

[52] K pojmu jiná závažná újma viz ŠÁMAL, Pavel a kol. *Trestnízákoník II. § 140 až 421. (Trestní zákoník II. § 140 až 421). Komentář k článku. (Komentář.)* 2. vydání. Praha: C. H. Beck, 2012, s. 1752-1753.
Konkrétně "*hrozba způsobení vážné újmy jinému může spočívat v hrozbě majetkové škody, vážné újmy na cti nebo pověsti atd.". Dalším typem vážné újmy může být zahájení trestního řízení v důsledku oznámení trestného činu, při němž pachatel vyhrožuje oběti tím, že ji nutí něco konat, něčeho se zdržet nebo něco strpět. Přitom není rozhodující, zda oběť spáchala trestný čin, jehož spácháním jí oznámení hrozí, či nikoli (srov. R 27/1982). "*

[53] Ke klasifikaci spamu srov. například GONZÁLES-TALAVÁN, Guillermo. Jednoduchý konfigurovatelný filtr spamu SMTP: Greylists. *Computers& Security*, 2006, roč. 25, č. 3, s. 229-236.

- Velmi účinnou formou podvodu jsou různé podvodné nabídky, které mohou být zasílány hromadně nebo cíleně. V současné době jsou takové nabídky zasílány nejen prostřednictvím e-mailu, ale také prostřednictvím všech druhů rychlých zpráv, sociálních sítí, aukčních webů atd.
- Pokud jde o **masové šíření** podvodných nabídek, lze si představit řadu "pyramidových" či "letadlových" aktivit, nabídek výhodné práce z domova[54] , "zaručených" metod zhodnocování (s nejvyššími úroky), nabídek půjček (s nejnižšími úroky), "skvělých" pracovních nabídek atd.
- **Cílené zasílání podvodných** nabídek by mělo zahrnovat i chování, které není pouhým spamem, ale například kombinací nabídky určitého typu zboží na aukčních portálech a následné komunikace s uživateli, kteří nabídku přijali. Tyto případy se označují jako "aukční podvody".
- **Možné trestní sankce v Polsku**
  V Polsku je zasílání nevyžádaných obchodních informací prostřednictvím elektronické komunikace považováno za přestupek, za který hrozí pokuta. Upravuje to zákon ze dne 18. července 2002 o poskytování služeb elektronickými prostředky (Dz. U. z roku 2002, č. 144, bod 1204):
- **Možné trestní sankce v České republice**
  Co se týče trestněprávních postihů za spam a spammery, nejsou v současné době v České republice zcela (vy)řešeny. Neexistuje žádná národní ani mezinárodní právní ochrana proti tomuto nežádoucímu jednání. Ani Úmluva o počítačové kriminalitě neobsahuje definici spamu jako trestného činu.
- **Možné trestní sankce v Portugalsku**
- Také v Portugalsku se obecně spam jako takový nepovažuje za trestný čin. Podle čl. 14 odst. 1 písm. f), g), h), i), j) zákona č. 41/2004 o ochraně údajů a soukromí v elektronických komunikacích však musí šiřitelé spamu pro komerční účely platit správní pokuty v minimální výši 1 500 EUR a maximální výši 50 000 EUR.

Phishing

- Termín phishing je nejčastěji definován jako podvodné nebo klamavé jednání, jehož cílem je získat informace o uživateli, jako je uživatelské jméno, heslo, číslo kreditní karty, PIN atd.
- V **užším slova smyslu je** phishing aktivita, která vyžaduje, aby uživatel navštívil podvodnou webovou stránku (zobrazující např. stránku internetového bankovnictví, internetového obchodu apod.) a poté vyplnil "přihlašovací údaje" nebo jsou tyto údaje přímo vyžadovány (např. při vyplňování formuláře apod.).
- V **širším slova smyslu** lze phishing definovat jako podvodné jednání, jehož cílem je vzbudit v uživateli důvěru, snížit jeho ostražitost nebo ho jinak donutit přijmout scénář předem připravený útočníkem.
- Princip "*klasického*" phishingového útoku obvykle spočívá v zaslání tzv. phishingového e-mailu oběti, který na první pohled nevzbuzuje žádné podezření, že by se mohlo jednat o podvodnou zprávu. Takový e-mail obvykle obsahuje odkaz, který uživatele přesvědčí, aby na něj kliknul.
- **Plánování phishingového útoku**

[54] Na jedné straně mohou tyto nabídky spočívat v požadavku, jako je např.: "*pošlete nám 10 dolarů na náš účet a my vám pošleme návod, jak vydělat 8 847 dolarů měsíčně*". Druhou možností je, že tyto nabídky práce nevyžadují žádnou platbu předem, vyžadují pouze registraci uživatele. Registrací útočník získá osobní údaje o uživateli. Na e-mailovou adresu uživatele pak může být zaslán e-mail od této společnosti, který obsahuje například malware apod.

V této fázi phishingového útoku je vybrán cíl (skupina uživatelů) a metoda, která bude použita pro útok. Posuzuje se, jaké technické zabezpečení cíl používá, jaké je riziko odhalení identity útočníka atd.

- **Vytvoření podmínek pro phishingový útok**

  V této fázi dochází k technickému řešení phishingového útoku. Útočník získá seznamy e-mailových adres uživatelů, kterým má být zaslán phishingový e-mail, vytvoří se datová schránka, do které systém odešle získané údaje o uživatelích, vytvoří se důvěryhodná zpráva, která je následně odeslána uživatelům.

- **Phishingový útok**

  Phishingový e-mail je doručen jednotlivým uživatelům a v závislosti na kvalitě zpracování tohoto e-mailu a dalších faktorech (zkušenosti uživatele, povědomí uživatele o problematice phishingu, antiphishingový software cíle atd.) je uživateli doručen phishingový e-mail. V této fázi phishingového útoku se uživatel setkává s phishingovým e-mailem poprvé.

- **Sběr dat**

  Útočník získá data, která jednotliví uživatelé napadeného systému zadali v prostředí falešné webové stránky.

- **Výběr finančních prostředků nebo jiných zisků z phishingového útoku**

  Na základě získaných údajů získá útočník přístup ke skutečným bankovním účtům jednotlivých uživatelů a vybere z nich finanční prostředky. Převodem na jiné, zejména zahraniční účty, rozředěním těchto prostředků a použitím dalších technik se vybrané prostředky stanou prakticky nedohledatelnými.

- **Možné trestní sankce v Polsku**

  Porušení tajemství komunikace (sniffing) čl. 267 § 3 trestního zákoníku. Tento typ trestného činu spočívá v získávání důvěrných informací, např. prostřednictvím snifferů, tj. programů, které zachycují data (hesla a uživatelská ID).

- **Možné trestní sankce v České republice**

  V případě kombinovaných forem phishingových útoků, kdy je k infikování počítače použit malware, musí být takové jednání pachatele trestáno také podle **§ 230** (Neoprávněný přístup k počítačovému systému a nosiči informací) trestního zákoníku. Pokud je cílem phishingového útoku získat pro sebe nebo jinou osobu neoprávněný prospěch, lze použít i ustanovení § **230 odst. 3 trestního** zákoníku.

- **Možné trestní sankce v Portugalsku**

  Vzhledem k tomu, že šíření škodlivého softwaru je trestné (čl. 6 odst. 2 zákona o kyberkriminalitě), jak bylo uvedeno, pouhé vytvoření neautentických údajů by bylo považováno za trestný čin počítačového padělání (čl. 3 zákona o kyberkriminalitě). Kromě toho, pokud by účelem takového vytvoření byl podvodný nebo nepoctivý záměr získat neoprávněně pro sebe nebo pro jinou osobu majetkový prospěch na úkor poškozeného, bylo by to rovněž považováno za počítačový podvod (článek 221 § 1 trestního zákona).

Pharming

- **Pharming**[55] je sofistikovanější a nebezpečnější forma phishingu. Jedná se o útok na server DNS (DomainName System), který převádí doménové jméno na IP adresu. K útoku dochází, když uživatel zadá do prohlížeče adresu webového serveru, na který chce přistoupit. Nepřipojí se však ke správné IP adrese původního webového serveru, ale k jiné, podvržené IP adrese.
- **Spearphishing** je jednou z forem phishingového útoku, ale rozdíl je v tom, že spearphishing je přesně cílený útok, na rozdíl od phishingu, který je spíše běžným (náhodným) útokem. Cílem útoku je obvykle konkrétní skupina, organizace nebo jednotlivec a konkrétně informace a data v rámci této organizace (např. duševní vlastnictví, osobní a finanční údaje, obchodní strategie, utajované informace atd.).
- **Možné trestní sankce v Polsku**
  Platí pro ně stejné zákony jako pro phishing.
- **Možné trestní sankce v České republice**
  Trest za spearphisher je podobný jako za phishing. Za spearphishingovým útokem může stát například teroristická organizace. V takovém případě není vyloučena odpovědnost za trestný čin podle **§ 311** (teroristický útok) trestního zákoníku.
- **Možné trestní sankce v Portugalsku**
  Závěr je stejný jako u phishingu obecně, včetně phishingu souvisejícího s terorismem.

Vishing

- Termín vishing[56] označuje telefonický phishing, při kterém útočník používá techniku sociálního inženýrství a pokouší se od uživatele získat citlivé informace (např. čísla účtů, přihlašovací údaje - jméno a heslo, čísla platebních karet atd.). Útočník se záměrně snaží zfalšovat jeho identitu. Útočníci se často vydávají za zástupce skutečných bank nebo jiných institucí, aby v uživateli vzbudili co nejmenší podezření. Vishing se používá při telefonování přes internet (VoIP).

Smishing

- Smishing[57] funguje na podobném principu jako vishing nebo phishing, ale k šíření zpráv využívá SMS zprávy. Smishing je v podstatě snaha přimět uživatele, aby zaplatil určitou částku (např. zavolal na bezplatnou linku, poslal dárcovskou SMS apod.) nebo kliknul na podezřelý odkaz URL. Pokud uživatel takovou adresu URL navštíví, je přesměrován na stránku, která zneužívá nějakou zranitelnost počítačového systému, nebo je uživatel vyzván k poskytnutí citlivých informací či malwaru.[58]

- **Možné trestní sankce v Polsku**

[55] Jedná se o spojení slov farmingi **phreaking**.
[56] Jedná se o kombinaci slov "voice" a "phishing".
[57] Jedná se o kombinaci slov "SMS" a "phishing".
[58] Např. Xshqi- *Android Worm na čínského Valentýna.* [online]. [citováno 14.8.2016]. Dostupné z: https://securelist.com/blog/virus-watch/65459/android-worm-on-chinese-valentines-day/
Selfmite- *Červ SMS pro Android Selfmite je zpět a je agresivnější než kdy dříve.* [online]. [citováno 14.8.2016]. Dostupné z: http://www.pcworld.com/article/2824672/android-sms-worm-selfmite-returns-more-aggressive-than-ever.html

Platí pro ně stejné zákony jako pro phishing.

- **Možné trestní sankce v České republice**
  Trestní postih za vishing a smishing je podobný jako za phishing.
- **Možné trestní sankce v Portugalsku**
  Závěr o kriminalizaci je opět stejný jako v případě phishingu obecně, včetně phishingu souvisejícího s terorismem.

Business Email Compromise (BEC)

- Kompromitace firemního e-mailu[59] je typ podvodného útoku, při kterém se útočník vydává za vedoucího pracovníka (obvykle generálního ředitele) a snaží se přimět zaměstnance, zákazníka nebo dodavatele, aby mu předal peníze nebo důvěrné informace.
- Oběťmi podvodu BEC se stávají malé podniky i velké společnosti. Podvody BEC jsou spojeny s dalšími formami podvodů, mimo jiné s podvody v oblasti romantiky, loterií, zaměstnávání a najímání zaměstnanců.
- Útočníci BEC spoléhají ve velké míře na taktiku sociálního inženýrství, aby oklamali nic netušící zaměstnance a manažery. Některé z ukázkových e-mailů mají předmět obsahující mimo jiné slova jako ***žádost***, ***platba***, ***převod*** a ***naléhavý.***

  Podvody typu BEC mají obvykle jednu z následujících forem:

1. **Podvod "CEO"**

   Útočníci předstírají, že jsou generální ředitel společnosti nebo jiný člen jejího vedení, a pošlou zaměstnancům podvržený e-mail s možností odeslat bankovní převod a pokynem, aby poslali finanční prostředky útočníkům.

2. **Falešné faktury**[60]

   Společnost, která má často s dodavatelem dlouhodobý vztah, je požádána, aby převedla finanční prostředky na úhradu faktury na jiný falešný účet. Útočník obvykle kontaktuje oběť prostřednictvím e-mailu nebo telefonu. E-mailový útok má obvykle upravený zdrojový kód (hlavičku) a předmět žádosti, takže vypadá velmi podobně jako legitimní žádost.

3. **Poškození účtu**

   Tento útok je podobný útoku Fake Invoice. Útočník použije e-mailový účet zaměstnance (hacknutý nebo podvržený) a poté odešle e-mail zákazníkům, ve kterém je informuje, že došlo k problému s jejich platbou a je třeba ji znovu zaslat na jiný účet.

4. **Vydávání se za podnikatele a právníky**

   Oběti jsou kontaktovány útočníky, kteří se představují jako právníci nebo zástupci advokátních kanceláří. Útočník žádá o převod velkého množství finančních prostředků na urovnání právního sporu nebo zaplacení nezaplaceného účtu. Útočník se snaží oběti přesvědčit, že převod je důvěrný a časově náročný, takže je méně pravděpodobné, že se zaměstnanec pokusí potvrdit, zda má finanční prostředky převést.

5. **Krádež dat**

   Typ BEC, jehož cílem není přímý převod peněz. Typickými oběťmi tohoto útoku jsou finanční nebo personální oddělení/zaměstnanci. Útočník je požádá o zaslání velmi citlivých údajů na

[59] Podvody BEC jsou známé také jako "CEO fraud" nebo "Man-in-the-Email".
[60] Útok je také označován jako: Útok se také nazývá "Schéma falešných faktur", "Podvod na dodavatele" a "Schéma úpravy faktur".

jejich účet. Používá se sociální inženýrství a útok na krádež dat může být výchozím bodem pro výše uvedené útoky BEC zaměřené na finanční převody.

- **Možné trestní sankce v Polsku**

  V Polsku to upravuje článek 286 (podvod), který říká, že:

  § 1. Kdo v úmyslu získat majetkový prospěch uvede jiného v nevýhodnou dispozici s vlastním nebo cizím majetkem tím, že uvede někoho v omyl nebo využije omylu nebo neschopnosti pochopit zamýšlené jednání, bude potrestán odnětím svobody na šest měsíců až osm let.

- **Možné trestní sankce v České republice**
  V České republice je možné výše popsané jednání postihnout podle **§ 209** (Podvod) trestního zákoníku. Doplňujícím trestným činem podvodu je obohacení. Vytvoření repliky webové stránky a získání přihlašovacích jmen a hesel by pak mohlo být kvalifikováno jako příprava nebo pokus trestného činu podle § 209 trestního zákoníku. Pokud by se útočník pokusil (§ 21 trestního zákoníku) získat pomocí získaných přístupových údajů neoprávněný přístup k účtu jiného uživatele, mohlo by být takové jednání rovněž kvalifikováno podle **§ 230** (Neoprávněný přístup k počítačovému systému a nosiči informací) trestního zákoníku.
- **Možné trestní sankce v Portugalsku**
  Jak již bylo vysvětleno v souvislosti s phishingem obecně, taková jednání by byla trestná jako počítačové padělání (článek 3 zákona o počítačové kriminalitě) a počítačový podvod (článek 221 trestního zákoníku).

Hacking

- Pojem hacking je v současné době veřejností vnímán pejorativně jako jakákoli činnost osoby, která chce získat nelegální přístup do cizího systému nebo osobního počítače.[61] Zejména v médiích se tento termín obecně používá pro označení jakéhokoli útočníka, jehož činnost je zaměřena proti informačním technologiím nebo jehož aktivity jsou založeny na využívání těchto technologií.
- Sami hackeři dnes používají termín hacker pro lidi, kteří mají vynikající znalosti systémů ICT, počítačových systémů, jejich operačních systémů a dalšího softwaru, principů a mechanismů sítí a jsou také vynikajícími programátory schopnými ve velmi krátké době vytvořit vlastní software.
- **<u>Rozdělení hackerů</u>**

  Právě motivace k získání neobvyklého (ne nutně nelegálního) přístupu, způsob provedení takového průniku, jejich motivace a případné nakládání se získanými údaji jsou klíčovými faktory pro rozdělení těchto osob do následujících tří hlavních skupin:

  Bílé klobouky *(***White** *Hats)* - jedná se o hackery, kteří pronikají do systému zneužíváním zranitelností v zabezpečení systému právě proto, aby tyto zranitelnosti odhalili a vytvořili takové mechanismy a bariéry, které by měly takovým útokům zabránit. Často se jedná o zaměstnance nebo externí spolupracovníky renomovaných společností působících v oblasti informačních technologií. Jejich průnik do systému nezpůsobuje uživatelům škody ani jiné újmy, naopak v mnoha případech upozorňují správce takto napadeného systému na bezpečnostní slabiny. Jejich činnost nemá v podstatě destruktivní charakter.

  Black Hast *(Černé klobouky)* - v podstatě opak hackerů s bílými klobouky. Jejich motivací je snaha způsobit uživateli napadeného systému škodu nebo jinou újmu, případně získat majetkový či jiný

[61] Podrobněji viz např. GRIFFITHS, Mark. Počítačová kriminalita a hackerství: vážný problém pro policii? *The Police Journal,* 2000, roč. 73, č. 1, s. 18-24.
YAR, Majid. Počítačové hackerství: jen další případ kriminality mladistvých? *The Howard Journal,* 2005, roč. 44, č. 4, s. 387-399.

prospěch. Kromě toho, že skutečně dosáhnou prolomení napadeného systému, je v jejich jednání patrný další kriminální prvek.

Grey Hats ***(Šedé klobouky)*** *- jedná se o* šedou zónu hackerů, tj. lidí, kteří se neprofilovali směrem k těmto dvěma skupinám. Občas mohou porušit některá práva druhých nebo morální zásady, ale jejich jednání není primárně diktováno snahou škodit, jako je tomu u černých klobouků.

- **Formy hackingu**
  Vlastní činnost hackerů se skládá z řady činností. Mezi typické činnosti hackerů patří:

  1. Sociální inženýrství
  2. Prolomení hesel[62]
  3. Skenování portů[63]
  4. Použití malwaru k infiltraci počítačového systému
  5. Phishing
  6. Cross Site Scripting[64]
  7. Odposlouchávání komunikace

- Pravděpodobně nejznámější hackerskou skupinou současnosti je Anonymous.

- **Možné trestní sankce v Polsku**
  Trestný čin hackerství je upraven v článku 267 § 1 trestního zákoníku.
- **Možné trestní sankce v České republice**
  Jak bylo uvedeno výše, existuje řada činností nebo útoků, které lze označit za hacking (od prolomení hesla až po sofistikované phishingové útoky kombinované se sociálním inženýrstvím a použitím malwaru).
  Jednání hackera, které spočívá pouze v tom, že využije svých schopností k překonání bezpečnostních opatření a získá přístup k počítačovému systému nebo jeho části, může být potrestáno podle § 230 odst. 1 (Neoprávněný přístup k počítačovému systému a nosiči informací) trestního zákoníku.

[62] Jedná se o proces získání hesla do počítačového systému. K prolomení hesel se běžně používají následující nástroje:
- Hádání hesel hrubou silou (testování hesel. dostatečně silné heslo je prevencí);
- Odhad hesla na základě znalosti uživatele (získané např. ze sociálních sítí apod.);
- Použití slovníku běžně používaných hesel (slovníkový útok);
- Vyžádání hesla od správce systému vydáváním se za oprávněného uživatele (Útočník se vydává za zapomenuté heslo a snaží se ho obnovit).
- zachycení hesel z nešifrované nebo nedostatečně šifrované síťové komunikace mezi počítačovým systémem a uživatelem.
- Vyhledávání hesel v datových souborech uložených systémem

[63] Jedná se o metodu, která zjišťuje otevřené síťové porty v počítačovém systému připojeném k počítačové síti. Na základě tohoto zjištění lze určit, jaké služby jsou v počítačovém systému spuštěny (např. webový server, ftp server atd.). Vlastní útok je pak zaměřen na zjištěné spuštěné služby na základě jejich zranitelnosti.

[64] Jedná se o útok, který spočívá v nabourání se do webové stránky. Tento typ útoku využívá aktivní prvky (skripty) na webové stránce, do kterých je vložen škodlivý kód a následně nabídnut oběti.
Jednou z méně obvyklých, ale o to nebezpečnějších činností je zneužití zranitelnosti webové aplikace ke spuštění malwaru v prohlížeči oběti. Oběť pak není schopna toto chování odhalit. Škodlivý kód funguje stejným způsobem jako zbytek webové stránky a útočník má možnost převzít v systému práva prohlížeče.
Podrobnější informace naleznete např. v *OWASP, XSS* [online] [citováno 15.7.2016]. Dostupné z: https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)

Cracking

- Pojem **cracking** je spojován s pojmem hacking, někdy jsou dokonce tyto pojmy veřejností nebo v médiích mylně zaměňovány. Z obsahového hlediska znamená pojem cracking prolomení nebo obejití ochranných prvků počítačového systému, programů nebo aplikací s úmyslem jejich následného neoprávněného použití.
- **Možné trestní sankce v Polsku**
  Platí stejné zákony jako v případě hackerství.

Možné trestní sankce v České republice

- Jednání pachatele, kterým je narušena ochrana počítačového systému nebo programu s úmyslem získat informace a následně je neoprávněně použít, naplňuje objektivní stránku trestného činu podle § 230 odst. 1 nebo 2 (Neoprávněný přístup k počítačovému systému a nosiči informací) trestního zákoníku. Pokud je cílem útoku crackem získat pro sebe nebo jinou osobu neoprávněný prospěch, lze použít i ustanovení § 230 odst. 3 trestního zákoníku.
- **Možné trestní sankce v Portugalsku**
  Nezákonný přístup do počítačového systému je trestný (čl. 6 odst. 1 zákona o počítačové kriminalitě). Kromě toho se jako objektivní znaky nevyžadují překonání bezpečnostních opatření a/nebo získání neoprávněné výhody, neboť se považují za přitěžující trestné činy (čl. 6 odst. 3 a 4).
  Jak již bylo uvedeno, nezákonné vytvoření, šíření nebo distribuce jakéhokoli počítačového programu, spustitelného pokynu, kódu nebo dat určených k provedení nezákonného přístupu do počítačového systému je trestné jako Nezákonný přístup (čl. 6 odst. 2 zákona o kyberkriminalitě), jako přitěžující trestný čin, pokud měl pachatel přístup k obchodnímu tajemství nebo důvěrným údajům, stejně tak v případě získání příslušné neoprávněné výhody (čl. 6 odst. 4 zákona o kyberkriminalitě).

Internetové pirátství

- Termín internetové pirátství je obecný pojem zahrnující trestné činy, které porušují práva duševního vlastnictví (velmi často se omezují na autorská práva). Teprve s rozšířením počítačových systémů a zejména s nástupem internetu můžeme hovořit o masovém pirátství jako o jedné z nejrozšířenějších forem počítačové kriminality.
- Právo duševního vlastnictví je nehmotný statek, tzv. hmotný statek, který je **výsledkem tvůrčí činnosti určité osoby**. Toto právo je **nezávislé na hmotném substrátu** (lze jej tedy použít kdykoli a kdekoli na světě) za předpokladu, že je **jedinečné, nereprodukovatelné a dostatečně originální.**
- Práva duševního vlastnictví lze rozdělit do dvou oblastí:
  1) **Autorské právo** (chrání např. původní literární a umělecká díla, hudební skladby, televizní vysílání, počítačové programy, databáze, reklamní výtvory, multimédia atd.).
  2) **Průmyslová práva** (chrání např. patenty na vynálezy, průmyslové vzory, průmyslové modely, ochranné známky, zeměpisný původ atd.).
- Nejčastěji používanými termíny jsou softwarové **pirátství** (s odkazem na porušování autorských práv k počítačovým programům) a **audiovizuální pirátství** (s odkazem na porušování autorských práv k audiovizuálním dílům - hudbě a filmu). **Základem softwarového a audiovizuálního pirátství je však vždy porušení některého z autorských práv nebo práv souvisejících s autorským právem.**
- Trestné činy proti duševnímu vlastnictví se s masovým nástupem internetu značně rozšířily. Mezi nejčastější případy porušování autorských práv v kyberprostoru patří:
  - *šíření díla e-mailem,* což je nejjednodušší způsob šíření malých souborů (zejména literárních nebo grafických autorských děl),

- *zveřejnění díla na webových stránkách* bez souhlasu autora. To je další velmi jednoduchý způsob, jak porušit autorská práva. Zveřejňovány jsou menší soubory (co do velikosti dat) a toto protiprávní jednání je obvykle velmi brzy odhaleno.
- *šíření díla nahráním na specializovaný server,* ze kterého lze díla volně stahovat (např. Megaupload, Rapidshare),
- *šíření díla prostřednictvím sítí P2P (Peer-to-Peer)*.[65] Tyto sítě jsou schopny přenášet/sdílet obrovské objemy dat (v řádu několika GB až desítek TB). Jedná se o nejkřiklavější případy porušování autorských práv.
- *zásahy do počítačových programů s cílem překonat technické prostředky držitele autorských práv, které brání vytváření kopií těchto chráněných programů* (tzv. crack),
- *šíření díla prostřednictvím datových nosičů přímo mezi uživateli (*půjčování a následné kopírování dat z DVD, HDD atd., prodej datových nosičů atd.),
- *nahrávání přímo během projekce a následné šíření záznamu (např.* nahrávání filmového díla přímo z plátna) - camcording,
- *neoprávněné předvádění audiovizuálních děl,*
- *skutečné pořízení počítačové práce*. Počítačový program je zvláště chráněn a podle autorského zákona není možné pořizovat kopie takového díla, a to ani pro osobní potřebu, bez souhlasu vlastníků autorských práv,
- *používání počítačového programu v rozporu s licencí,*

- **Umístění díla** (audiovizuálního nebo softwarového) v kyberprostoru (**upload)** představuje šíření díla ve smyslu autorského zákona a (pokud k tomu autor nebo jiná oprávněná osoba nedá svolení) může být trestné. **Neoprávněným užitím díla je rovněž zveřejnění odkazu na místo v kyberprostoru, odkud lze dílo získat.**

Warez

- Pojem "warez" se často objevuje v souvislosti s internetovým pirátstvím. Warez **je zjednodušeně** řečeno **forma softwarového pirátství, kdy** informační technologie slouží pouze jako prostředek k urychlení šíření nelegálních kopií autorsky chráněných děl prostřednictvím internetu. Warezová fóra se v současné době využívají především ke stahování cracků a keygenů, ale i kompletně upravených programů, filmů a hudby. Konečný produkt warezové scény se nazývá **release**.
- **Možné trestní sankce v Polsku**
  Problematiku duševního vlastnictví v Polsku upravují dva základní právní předpisy: zákon o autorském právu a právech s ním souvisejících a zákon o právu průmyslového vlastnictví.
- **Možné trestní sankce v České republice**
  Sdílení souborů, ať už na warezových nebo P2P sítích, může být trestné podle § **270** (Porušování autorského práva, práv souvisejících s autorským právem a práv k databázi) nebo podle **§ 231** (Prostředky a uchovávání přístupových zařízení k počítačovému systému a hesel a jiných podobných údajů) trestního zákoníku.
- **Možné trestní sankce v Portugalsku**
  Obecně je takové jednání trestné jako neoprávněné kopírování, šíření a prodej děl a/nebo jako padělání autorských děl (články 195 a 196 zákoníku o autorském právu a právech s ním souvisejících).

[65] Připojením k P2P začne uživatel ve výchozím nastavení automaticky sdílet svůj obsah s ostatními (obvykle neznámými) uživateli. Obvykle se při stahování automaticky nastaví odesílání staženého materiálu.

Sniffing

- Sniffing je metoda nelegálního zachycení dat procházejících počítačovou sítí během komunikace mezi poskytovanou službou a počítačovým systémem pomocí **snifferu.**[66]
- **Možné trestní sankce v Polsku**
  V Polsku je čichání (sniffing) trestným činem, který se trestá podle:
  Porušení tajemství komunikace (čmuchání) § 267 odst. 3 TZ.
- **Možné trestní sankce v České republice**
  Takové jednání lze prakticky označit za **nezákonný odposlech a záznam telekomunikačního provozu**. Výše popsané jednání zcela jistě zasahuje do základních lidských práv a svobod, zejména do **článku 13 Listiny, a je zcela lhostejné, zda nezákonné odposlouchávání provádí externí útočník nebo správce sítě.** Podle trestněprávních norem by bylo možné takové jednání podřadit pod **§ 182 odst. 1 (**Porušení tajemství dopravovaných zpráv) trestního zákoníku a v případě zneužití takto získaných informací by se mohlo jednat o trestný čin podle **§ 182 odst. 2** trestního zákoníku
- **Možné trestní sankce v Portugalsku**
  Takové jednání spadá do oblasti působnosti nezákonného odposlechu (článek 7 zákona o kyberkriminalitě), ale také sdílení a zpřístupnění jakéhokoli obsahu může být považováno za Porušení listovního nebo telekomunikačního tajemství (článek 194 trestního zákoníku).

DoS

- Termín DoS je zkratkou pro "***odepření služby"***. Jedná se o jednu z forem útoku na (internetovou) službu, jejímž cílem je vyřadit nebo snížit výkon napadeného technického zařízení.[67] Tento útok je prováděn zahlcením napadeného počítačového systému (nebo síťového prvku) opakovanými požadavky na provedení akce.
- Rozdíl mezi útoky DoS, DDoS a DRDoS spočívá především ve způsobu provedení útoku. Pro přehlednost jsou jednotlivé typy útoků doplněny nákresy znázorňujícími způsob provedení útoku.
- V případě **DoS (Denial of Service)** je zdroj útoku jeden. Proti tomuto typu útoku se lze poměrně snadno bránit, protože je možné zablokovat provoz ze zdroje útoku.
- Při **distribuovaném odepření služby (DDoS)** je cílový počítačový systém přetížen **odesíláním paketů z více počítačových systémů na různých místech, což ztěžuje obranu a identifikaci útočníka**. Tento typ útoku byl použit například proti společnosti Yahoo! Inc, elektronickému obchodu atd.[68] K tomuto typu útoku jsou velmi často využívány botnety nebo akce uživatelů podporujících určitou internetovou kampaň (viz dále - Anonymous a LOIC). v případě **DRDoS (Distributed ReflectedDenial of Service)** se jedná o spoofedDoSattack, který využívá tzv. reflection mechanismus. Útok spočívá v zasílání falešných požadavků na připojení velkému počtu počítačových systémů, které pak na tyto požadavky odpovídají, ale nikoli iniciátorovi připojení, ale oběti.

---

[66]Sniffing je anglický výraz pro slídění nebo špehování. Sniffer je tedy někdo, kdo slídí, čmuchá nebo špehuje.

[67] Podrobněji např. MARCIÁ-FERNANDÉZ, Gabriel, Jesús E. DÍAZ-VERDEJO a Pedro GARCÍA-TEODORO. Vyhodnocení útoku DoS s nízkou rychlostí proti aplikačním serverům. *Computers & Security*, 2008, roč. 27, č. 7-8, s. 335-354.
CARL, Glenn, Richard BROOKS a Rai SURESH. Wavelet-Based Denial-of-Service Detection. *Computers & Security*, 2006, roč. 25, č. 8, s. 600-615.
RAK, Roman a Radek KUMMER. Informačníhrozby v letech 2007-2017. *security magazín*, 2007, roč. 14, č. 1, s. 3.

[68] Například útoky DoS na webové stránky předsednictví, parlamentu, ministerstev, médií a dvou estonských bank - Estonsko (2007). *Estonsko se vzpamatovává z masivního DDoS útoku.* [online]. [cit. 4. 3.2010] Dostupné na: http://www.usatoday.com/tech/news/techpolicy/2007-09-12-spammer-va_N.htmhttp://www.computerworld.com/s/article/9019725/Estonia_recovers_from_massive_DDoS_attack

- Útoky DoS, DDoS, DRDoS velmi často zneužívají chyby v operačním systému, běžících programech nebo síťových protokolech - UDP, TCP, IP, http atd.
- Existuje několik základních metod útoku DoS nebo DDoS, z nichž nejznámější jsou:

  Zaplavení příkazem ping (*Ping-Flood*)

  Díky protokolu Internet Control Message Protocol a nástroji Ping (Packet Internet Groper) je možné pomocí příkazu "ping" zjistit "životnost" počítačového systému s danou IP adresou a zjistit dobu odezvy takového systému.

  Zaplavení volných systémových prostředků (*SYN-Flood*)

  SYN-Flood je typ útoku, při kterém se útočník snaží zahltit oběť velkým počtem požadavků na připojení. Útočník posílá cílovému počítačovému systému (oběti) sekvenci příkazových paketů SYN (SYN pakety), přičemž cílový systém na každý paket SYN reaguje zasláním paketu SYN-ACK, ale útočník již neodpovídá.

  Podvržení **zdrojové adresy** (*IP spoofing*)

  IP Spoofing je podvržení zdrojové adresy odesílaných paketů, kdy útočník iniciující spojení ze stroje A s IP adresou a.**b.c.**dw nastaví jako zdrojovou adresu např. IP adresu **d.c.b.**ai a odešle ji cíli B. Cíl B na tuto zdrojovou adresu odpoví, tj. odpověď nesměřuje na IP adresu a.b.c.d, ale na IP adresu **d.c.b.a.**

  Šmoulí útok

  Tento útok se provádí chybným nastavením systému tak, aby odesílal pakety všem počítačům připojeným k počítačové síti prostřednictvím vysílací adresy.

- Cílem útoků DoS/DDoS obvykle **není infikovat počítač** nebo počítačový systém, **ani překonat bezpečnostní prvky hesla, které jej** chrání, ale **zahltit jej nebo dočasně vyřadit z provozu** sérií opakovaných požadavků. Výsledkem je obvykle omezení nebo zablokování přístupu ke službám.
- **Možné trestní sankce v Polsku**
  V tomto případě se použije článek 268 trestního zákoníku.
- **Možné trestní sankce v České republice**

  Vyplývá to ze znění ustanovení článku **230 odst. 2** (Neoprávněný přístup k počítačovému systému a nosiči informací) trestního zákoníku:

  Kdokoli získá přístup k počítačovému systému nebo paměťovému médiu a

  (a) neoprávněně použije data uložená v počítačovém systému nebo na paměťovém médiu, (b) neoprávněně smaže nebo jinak zničí, poškodí, změní, potlačí nebo poškodí kvalitu dat uložených v počítačovém systému nebo na nosiči informací nebo je učiní nepoužitelnými.....

  Z tohoto ustanovení vyplývá, že útočník, který se dopustí útoku DoS nebo DDoS, musí získat neoprávněný přístup do počítačového systému a následně v něm potlačit data, aby mohl být trestně odpovědný.[69]

- **Možné trestní sankce v Portugalsku**
  Takové činy nepochybně spadají do oblasti působnosti počítačové sabotáže [nezákonný zásah] (čl. 5 odst. 1 zákona o kyberkriminalitě), případně jako přitěžující trestný čin v případě závažného poškození nebo narušení kritické infrastruktury nebo jiných základních služeb (čl. 5 odst. 5).

  Šíření nežádoucího obsahu
- V současné době lze popsat dva základní typy šíření nežádoucího obsahu. Šíření zakázaných typů pornografie a šíření nenávistného a extremistického obsahu.
- **Možné trestní sankce v Polsku**

[69]Potlačením se rozumí činnost uvedená v článku 4 Úmluvy o počítačové kriminalitě.

V Polsku platí následující článek trestního zákoníku:
Článek 200b. Veřejná propagace pedofilního obsahu
Článek 202 Prezentace a šíření pornografie

- **Možné trestní sankce v České republice**
  V případě vytvoření, držení nebo šíření materiálu spadajícího pod pojem dětská pornografie je možné uživatele potrestat podle **§ 192** (Výroba a jiné nakládání s dětskou pornografií), § **193** (Využití dítěte k výrobě pornografie) trestního zákoníku. Trestným činem je rovněž účast na pornografickém nebo jiném podobném představení s účastí dítěte (**§ 193a trestního zákoníku)**. Trestným činem je rovněž přístup k dětské pornografii prostřednictvím informačních nebo komunikačních technologií (§ **192 odst. 2 trestního zákoníku)**.
- **Možné trestní sankce v Portugalsku**
  Takové činy jsou v závislosti na případu trestněprávně postihovány různě. Na jedné straně mohou být považovány za trestné činy související s dětskou pornografií (§ 176 TZ). Na druhé straně představují závažné narušení soukromí (čl. 191 odst. 1 písm. b) a 197 písm. b) trestního zákoníku) nebo jako pornografii z pomsty související s domácím násilím (čl. 152 odst. 2 písm. b) trestního zákoníku (čl. 193() trestního zákoníku).

Kybernetické útoky na platformy sociálních médií

- V rámci sociálních médií je možné spáchat většinu dříve popsaných kybernetických útoků (např. malware, phishing, spam atd.). Důvodem, proč byly kybernetické útoky na platformách sociálních médií popsány samostatně, je skutečnost, že k nim dochází především (ale ne výhradně) v prostředí sociálních médií.
- Kyberšikana pak přesouvá "klasickou šikanu" do virtuálního světa a umožňuje útočníkovi používat nástroje a prostředky, které mohou mít na oběť mnohem větší dopad než v reálném světě. Kyberšikana díky využití informačních a komunikačních technologií a přetrvávání dat v kyberprostoru umožňuje opakované útoky na oběť, a to i v případě, že se oběť v reálném světě geograficky vzdálila od místa, kde byla původně obtěžována.
- **Nejčastější projevy kyberšikany:**
  Pomlouvání, šikanování, urážení, zesměšňování nebo jiné ztrapňování (sociální sítě, e-mail, SMS, chat, ICQ, Skype, hry atd.).

  Pořizování zvukových záznamů, videozáznamů nebo fotografií, jejich grafické nebo jiné zpracování a následné zveřejnění s cílem poškodit (zesměšnit) vybranou osobu.

  natáčení videí, v nichž je oběť fyzicky napadána nebo jinak psychicky týrána a zesměšňována. Tato videa jsou pak zveřejňována na internetu (jedná se o tzv. Happy Slapping).

  Vytváření webových stránek, účtů na sociálních sítích (úprava původních nebo vytváření nových profilů), diskusních stránek atd., které urážejí, očerňují nebo ponižují konkrétní osobu.

  Zneužití cizího účtu - krádež identity (e-mail, diskuse atd.).

  Provokování a napadání uživatelů v diskusních fórech (chatech atd.).

  Odhalování cizích tajemství.

  Vydírání pomocí mobilního telefonu nebo internetu.

  Obtěžování a pronásledování voláním, psaním zpráv.

- **Možné trestní sankce v Polsku**
  V Polsku se tato oblast řídí:
  § 212 OZ - pomluva a § 190 odst. 1

- **Možné trestní sankce v České republice**
  Kyberšikana (stejně jako klasická šikana) není sama o sobě trestným činem ani přestupkem. Vždy záleží na jednání obtěžujícího. Pokud by takové jednání mělo formu například fyzického ublížení oběti, vydírání nebo zastrašování, pak by bylo možné uvažovat o aplikaci například § 146 (Ublížení na zdraví) nebo § 145 (Těžké ublížení na zdraví), § 175 (Vydírání) trestního zákoníku. V případě obtěžování a trestního stíhání osoby by bylo možné použít § 354 trestního zákoníku (nebezpečné pronásledování).
- **Možné trestní sankce v Portugalsku**
  Kyberšikana jako taková není trestným činem. Lze ji však považovat za formu stalkingu (§ 154-A trestního zákoníku), ale také za sexuální obtěžování, urážku, pomluvu, závažný zásah do soukromí, a dokonce i za diskriminaci a podněcování k nenávisti a násilí (§ 154-A trestního zákoníku). 170, 181, 180, 192 a 197 písm. b) a 240, vše trestního zákoníku).

Kybergrooming

- Kybergrooming je psychická manipulace s osobou (obvykle pomocí sociálního inženýrství), která se provádí prostřednictvím internetu nebo informačních a komunikačních technologií (např. mobilních telefonů atd.). Cílem kybergroomingu je vzbudit v oběti falešnou důvěru a vyvolat tak osobní schůzku. Výsledkem takového setkání může být jakýkoli fyzický, sexuální nebo jiný útok na oběť. Obětí kybergroomingu se mohou stát děti i dospělí. Podle statistik jsou nejčastějšími oběťmi dívky ve věku 13 až 17 let.
- **Možné trestní sankce v Polsku**
  V červnu 2010 vstoupila v platnost novela trestního zákoníku. V trestním zákoníku se objevil zcela nový druh trestného činu, upravený v § 200a TZ, tzv. grooming, tj. svádění prostřednictvím internetu. Týká se osob, které prostřednictvím informačního a komunikačního systému nebo telekomunikační sítě naváží kontakt s nezletilou osobou mladší 15 let s cílem uvést ji v omyl, využít jejího omylu či neschopnosti správně pochopit situaci nebo jí protiprávně vyhrožovat schůzkou. Za tento trestný čin hrozí trest odnětí svobody až na tři roky.

- **Možné trestní sankce v České republice**
  Osoba, která se dopouští kybergroomingu, může svým jednáním naplnit objektivní znaky některých trestných činů uvedených v trestním zákoníku. Zpravidla půjde v závislosti na povaze jednání útočníka o trestné činy podle ustanovení § 168 (Obchodování s lidmi), § 171 (Neoprávněné zbavení osobní svobody), § 175 (Vydírání), § 185 (Znásilnění), § 187 (Pohlavní zneužívání), § 201 (Ohrožování výchovy dítěte), § 209 (Podvod), § 353 (Nebezpečné vyhrožování), § 354 (Nebezpečné pronásledování) trestního zákoníku.
- **Možné trestní sankce v Portugalsku**
  Nabádání dětí k sexuálním účelům prostřednictvím informačních a komunikačních technologií je trestným činem (článek 176-A trestního zákoníku).

Sexting

- Jednou z forem nebezpečného chování, zejména v prostředí sociálních sítí, je tzv. sexting. Termín sexting vznikl spojením slov sex a textová zpráva. Jedná se o elektronické šíření textových zpráv, fotografií nebo videí se sexuálním obsahem.

- **Možné trestní sankce v Polsku**

  Podle polských zákonů je zakázáno:

  - výroba pro šíření;
  - nahrávání;
  - šíření;
  - prezentace;
  - držení a skladování;
  - Dovoz

  pornografický materiál za účasti nezletilé osoby - osoby mladší 18 let (§ 202 TZ).

- **Možné trestní sankce v České republice**
  Pokud jsou fotografie jiné osoby zveřejněny bez jejího souhlasu, může se domáhat svých práv v občanskoprávním řízení.
- **Možné trestní sankce v Portugalsku**
  Zasílání takového obsahu jiné dospělé osobě může být stíháno jako sexuální obtěžování (§ 170 TZ). Pokud však někdo zašle takový obsah třetí osobě, bude to považováno za pomluvu, útrpné narušení soukromí, útrpné domácí násilí nebo dokonce za diskriminaci a podněcování k nenávisti a násilí (§ 180, 152, 192 a 197 písm. b) a 240, všechny trestního zákoníku).

Kyberstalking

- Kyberstalking je opakované kontaktování oběti, např. prostřednictvím textových zpráv, e-mailů, telefonátů, VoIP, instant messagingu atd. Jednání útočníka se obvykle stupňuje a obvykle vyvolává obavy o soukromí, zdraví nebo život oběti.
- Kyberstalker se vyznačuje vytrvalostí a systematičností a není neobvyklé, že si vytvoří několik falešných identit, pod kterými oběť kontaktuje.
- Kyberstalker může také demonstrovat svou moc a sílu, například zveřejněním informací o životě oběti, které může získat z různých internetových zdrojů.
- **Možné trestní sankce v Polsku**
  Podle polského trestního zákoníku lze stalking spáchat dvěma způsoby. Vytrvalým obtěžováním potrestané osoby (článek 190a § 1 trestního zákoníku) nebo vydáváním se za jinou osobu (článek 190a § 2 trestního zákoníku). Kvalifikace konkrétního jednání jako stalkingu závisí na tom, zda pachatel splňuje několik podmínek.
- **Možné trestní sankce v České republice**
  Stalking nebo kyberstalking může za určitých podmínek spadat pod **§ 354** (Nebezpečné pronásledování) trestního zákoníku. Mezi základní podmínky patří, že stalker musí oběť "*vytrvale* kontaktovat *elektronickými, písemnými nebo jinými prostředky" po delší dobu* a takové jednání je způsobilé vyvolat důvodnou obavu o život nebo zdraví oběti nebo život a zdraví jejích blízkých. Přitěžující okolností podle **§ 354 odst. 2 písm. a)** trestního zákoníku je, pokud byl uvedený čin spáchán ke škodě dítěte.
- **Možné trestní sankce v Portugalsku**
  V poslední době se stalking, včetně kyberstalkingu, stal trestným činem jako pronásledování (článek 154-A trestního zákoníku).

Krádež identity

- Krádež identity je útok, při kterém je odcizena virtuální identita[70] , nebo se jedná o převzetí kontroly (trvalé či dočasné) nad touto identitou. Motivem útočníka může být finanční zisk, ale i další výhody související s tím, že útočník jedná jménem jiné osoby, např. přístup k informacím o jiných osobách, přístup k firemním datům apod.
- **Možné trestní sankce v Polsku**
  Podle § 190a odst. 2 trestního zákoníku, kdo se vydává za jinou osobu a zneužije její podobizny nebo jiných osobních údajů k tomu, aby jí způsobil majetkovou nebo osobní újmu, bude potrestán odnětím svobody až na tři léta.
- **Možné trestní sankce v České republice**
  Pokud dojde k překonání zabezpečení a neoprávněnému přístupu k identitě oběti, dojde k naplnění skutkové podstaty trestného činu podle **§ 230 odst. 1 (**Neoprávněný přístup k počítačovému systému a nosiči informací) trestního zákoníku. Použitím škodlivého softwaru za stejným účelem se útočník dopustí trestného činu podle § 230 odst. 2 trestního zákoníku. Pokud je účelem krádeže identity získat pro sebe nebo jinou osobu neoprávněný prospěch, může se uplatnit i ustanovení § **230 odst. 3** trestního zákoníku. Pokud útočník odcizí identitu s cílem uvést jinou osobu v omyl, tj. uvést někoho v omyl za účelem vlastního obohacení, může být takové jednání posouzeno rovněž podle **§ 209** (Podvod) trestního zákoníku
- **Možné trestní sankce v Portugalsku**
  Vydávání se za někoho jiného již není trestné. Vytváření neautentických údajů pro právně relevantní účely by však bylo považováno za počítačové padělání (článek 3 zákona o počítačové kriminalitě). Dále, pokud by účelem takového vydávání se za někoho jiného byl podvodný nebo nečestný záměr získat pro sebe nebo jinou osobu neoprávněně majetkový prospěch na úkor poškozeného, jednalo by se rovněž o počítačový podvod (čl. 221 odst. 1 trestního zákona).

APT

- APT je zkratka pro pokročilé a trvalé hrozby. Jedná se o trvalý systematický kybernetický útok zaměřený na cílový počítačový systém nebo ICT cílové organizace. K takovému útoku se používají různé techniky a poměrně velké prostředky a obvykle mohou být napadeny sekundární cíle (např. počítačové systémy, např. opakované DoS nebo jiné útoky), aby se odvedla pozornost od primárního cíle (infiltrace společnosti malwarem), na který se následně útočí.
- Během útoku APT mohou útočníci na vybraný cíl použít další různé typy útoků v závislosti na získaných datech a informacích.
- **Možné trestní sankce v Polsku**
  Při analýze útoku APT z hlediska porušení platných právních předpisů v Polsku je třeba uznat, že pokud by byl útok proveden ve všech jeho fázích, došlo by ke spáchání přinejmenším několika trestných činů. Podle platného práva lze útok APT považovat za:

[70] Virtuální identitou se rozumí jakákoli identita nebo avatar, který osoba používá k interakci v kyberprostoru (např. e-mail, účet na sociální síti, hra, různá online tržiště, počítačový systém atd.). Nezáleží na tom, zda je virtuální identita skutečná nebo falešná, tj. zda představuje skutečnou osobu, nebo zda se jedná o zcela uměle vytvořenou identitu bez reálného základu.

- hacking podle článku 267 § 1 trestního zákoníku.
- trestný čin výroby a poskytování počítačových zařízení nebo programů, hesel a kódů podle článku 269b trestního zákoníku.
- počítačový podvod podle článku 287 trestního zákoníku.

- **Možné trestní sankce v České republice**
  Případný trestní postih útočníka (útočníků) provádějícího útok APT pak zcela závisí na jeho jednání, které může mít například podobu šíření malwaru, některého z phishingových útoků, krádeže identity atd.
- **Možné trestní sankce v Portugalsku**
  Útok APT není výslovně trestný, a to ani jako přitěžující trestný čin.

Terorismus

- Terorismus lze podle formy rozdělit na *smrtící* a *nesmrtící formy,* přičemž první skupina se vyznačuje použitím běžně dostupných násilných prostředků (*konvenční* - útoky spáchané běžně dostupnými zbraněmi, jako jsou střelné zbraně, a nekonvenční - zneužití zbraní hromadného ničení). Naproti tomu nesmrtící **formy terorismu**[71] nebo útoky využívající modernější nástroje v kombinaci se smrtícími prostředky jsou častější online.
- Konvenční forma nesmrtícího terorismu zahrnuje následující podskupiny:

  - *Neozbrojený terorismus*.

  - Kyberterorismus - jedna z největších hrozeb 21. století. Principem je především zneužití informačních a komunikačních technologií (včetně internetu) jako prostředku a prostředí k provedení útoku. Stejně jako v případě klasického konvenčního teroristického útoku jde o plánovanou činnost, obvykle politicky nebo nábožensky motivovanou a prováděnou spíše malými než vojensky organizovanými strukturami.

Mediální terorismus, při kterém dochází k plánovanému zneužití médií a dalších psychologických zbraní k ovlivnění názorů obyvatelstva nebo cílových skupin.

- **Možné trestní sankce v Polsku**
  V Polsku se na provedení kyberteroristického útoku vztahují články 265 až 269 a článek 287 trestního zákoníku a v závislosti na účinku kyberteroristického útoku se mohou použít i některé další články trestního zákoníku, např:
  Článek 163 Způsobení katastrofy
  Článek 164 Způsobení nebezpečí katastrofy
  Článek 165 Způsobení veřejného nebezpečí
  Článek 173 Způsobení dopravní nehody
  Článek 174 Způsobení bezprostředního nebezpečí dopravní katastrofy
- **Možné trestní sankce v České republice**
  Z hlediska trestního práva mohou výše uvedené skutky naplňovat objektivní znaky trestných činů podle § 311 odst. 2 (teroristický útok), § 355 (hanobení národa, rasy, etnické nebo jiné skupiny osob), § 356 (podněcování k nenávisti vůči skupině osob nebo potlačování jejich práv a svobod), § 364 (podněcování k trestnému činu), § 403 (vytváření, podpora a propagace hnutí směřujících k

[71] Lze si však představit i kombinaci těchto útoků. Podrobnější informace lze nalézt např. v:
Exkluzivně: Počítačový virus zasáhl flotilu amerických dronů. [online]. [cit. 10.7.2016]. Dostupné z: https://www.wired.com/2011/10/virus-hits-drone-fleet/.

potlačení práv a svobod člověka) a § 404 (projevování sympatií k hnutí směřujícímu k potlačení práv a svobod člověka) trestního zákoníku.

- **Možné trestní sankce v Portugalsku**
  Podle protiteroristického zákona č. 52/2003 se v případě, že trestné činy souvisejí s teroristickými účely, zvyšují tresty za trestné činy, jako je počítačový podvod nebo počítačové padělání, o jednu třetinu (čl. 4 odst. 2). Kromě toho se zpřísňují tresty za trestné činy související s elektronickou komunikací (čl. 4 odst. 3 bod 4), náborem (čl. 4 odst. 5 bod 6) nebo propagací teroristických skupin nebo činností, pokud byly spáchány prostřednictvím internetu (čl. 4 odst. 8 bod 9).

3. Během výuky

<u>Několik nápadů na aktivity:</u>

WORKSHOPY

1. Analýza jednotlivých kybernetických útoků a jejich subsumpce pod ustanovení Úmluvy o kyberkriminalitě (ESD č. 185) a vnitrostátní právo (Česká republika, Polsko, Portugalsko).
2. Analýza jednotlivých útoků - modus operandi
3. Testování zabezpečení proti vybraným útokům.
4. Definice možností prevence jednotlivých typů útoků
5. Návrh řešení na míru pro ochranu před jednotlivými kybernetickými útoky.
6. testování bezpečnosti některých systémů, aplikací a dat. Studenti se pokusí navrhnout vlastní řešení pro zvýšení bezpečnosti těchto systémů, aplikací nebo dat.
7. Seznámení s nástroji a prostředky pro bezpečné ukládání dat a nastavení bezpečné online komunikace (např. správa a nastavení VPN, PGP, správce hesel atd.).

KONTROLNÍ OTÁZKY

1.

- Co je kyberkriminalita?
- Co není kybernetický zločin?
- Co je to kybernetický útok?
- Jaký je rozdíl mezi kybernetickou kriminalitou a kybernetickým útokem?
- Jaký je rozdíl mezi daty a informacemi?
- Co je triáda CIA?

2.

- Co je charakteristické pro sociální inženýrství?
- Co je botnet a jak funguje?
- Jaké jsou typické topologie botnetů?
- Může být vlastnictví botnetu považováno za trestný čin?
- Co je to malware?
- Jaké jsou nejčastější příklady malwaru?
- Jaké jsou nejčastější vektory infekce malwarem?

- Co je ransomware a jaké jsou jeho projevy?
- Co je to phishing a jak se tento útok nejčastěji provádí?
- Jaký je rozdíl mezi phishingem a pharmingem?
- Co je to hacking?
- Co je charakteristické pro praskání?
- Jaký je rozdíl mezi hackingem a crackingem?
- Co je útok DoS a jak funguje?
- Jaký je rozdíl mezi DoS a DDoS?
- Co lze zahrnout do distribuce závadného obsahu?
- Co je APT?

Práce ve dvojicích/skupinách

- **Dvojice - miniprojekt**
  Studenti si ve dvojicích vyberou jedno z probíraných témat. Zapíší své závěry a představí je ostatním. Po prezentaci si ostatní studenti připraví doplňující otázky pro prezentující skupinu.

- **Myšlenková mapa**
  Studenti si ve dvojicích vyberou jedno z probíraných témat a vytvoří myšlenkovou mapu, kterou pak v krátké prezentaci popíší ostatním studentům.

- **Klíčová slova**
  Studenti ve dvojicích samostatně vyberou klíčová slova ze slovníčku.

  Definice těchto slov napíší na proužky papíru. Proužky otočí prázdnou stranou nahoru. Jeden student si vybere proužek, přečte definici a druhý student hledá odpovídající klíčové slovo.
  nebo
  Studenti si na papír napíší několik klíčových slov ze slovníčku. Kartičky otočí prázdnou stranou nahoru. Jeden student si vezme první kartičku a řekne, co dané slovo znamená. Druhý student klíčové slovo hádá.

- 10 klíčových slov
  Studenti si vyberou 10 klíčových slov souvisejících s vybraným tématem. Těchto 10 klíčových slov předají ostatním dvojicím. Dvojice napíší text, který musí obsahovat všechna klíčová slova. Jedna věta může obsahovat pouze jedno klíčové slovo. Text se tedy skládá minimálně z 10 vět.

- Panelová diskuse

  Studenti si vyberou 3 řečníky. Každý řečník si vybere jedno téma, o kterém bude diskutovat. Ostatní studenti kladou otázky k tématům. Každý mluvčí může použít typ odpovědi -PRAVDA X NEPRAVDA. Za každou pravdivou odpověď získá student bod, např. znamená GDPR GENERAL DATA PROTECTION REGULATION? - PRAVDA X NEPRAVDA.

4. Internetové zdroje

Viz bibliografie níže

5. Další otázky/testy

VYBERTE SPRÁVNOU ODPOVĚĎ:
(Správná odpověď byla zvýrazněna)

1. _____ lze definovat jako chování namířené proti počítači nebo v některých případech proti počítačové síti nebo jako chování, při kterém je počítač použit jako nástroj ke spáchání trestného činu.

   a) Kybernetický hacking
   b) Kybernetický efekt
   (c) Kybernetický útok
   d) Kyberkriminalita

2. _____ lze definovat jako jakékoli protiprávní jednání útočníka v kyberprostoru, které je namířeno proti zájmům jiné osoby.

   a) Kybernetický incident

   (b) Kybernetický útok

   d) Kybernetická nehoda

   (c) Cybernapad

3. Počítač _____ znamená "jakékoli vyjádření faktů, informací nebo pojmů ve formě vhodné pro zpracování v počítačovém systému, včetně programu schopného přimět počítačový systém k provedení určité funkce".

   (a) pojmy

   (b) pokyny

   (c) časové lhůty

   (d) údaje

4. _____ je "narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti poskytování služeb nebo narušení bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické události".

   (a) kybernetická bezpečnostní kriminalita
   b) Dosažení kybernetické bezpečnosti
   c) Oslabení kybernetické bezpečnosti
   (d) Incident kybernetické bezpečnosti

5. _____ je "událost, která má potenciál ohrozit bezpečnost informací v informačních systémech nebo ohrozit bezpečnost služeb či bezpečnost a integritu sítí elektronických komunikací".

(a) Incident v oblasti kybernetické bezpečnosti
b) Skandál v oblasti kybernetické bezpečnosti
c) Zanedbání kybernetické bezpečnosti
d) Otázka kybernetické bezpečnosti

6. _____ nelze považovat za přímo použitelný v celém rozsahu pro kybernetický útok, ale je podmínkou úspěchu mnoha kybernetických útoků.

(a) stavební inženýrství
(b) sociální inženýrství
(c) kybernetické inženýrství
(d) trestní inženýrství

7. _____ lze nejjednodušeji definovat jako síť softwarově propojených botů, kteří provádějí určitou akci na základě příkazu "vlastníka" (nebo správce) této sítě.

(a) Bennet
(b) Maska
(c) Botnet
(d) Bootnet

8. _____ jsou obecně takové počítačové programy, které obsahují skryté funkce, s nimiž uživatel nesouhlasí nebo o nichž neví a které jsou potenciálně nebezpečné pro další fungování systému.

a) Krádež dat
(b) Pharming
c) Rootkity
(d) trojské koně

9. Termín _____ se nejčastěji používá k popisu podvodného nebo klamavého chování, jehož cílem je získat informace o uživateli, jako jsou uživatelská jména, hesla, čísla kreditních karet, PIN kódy atd.

(a) phishing
(b) spyware
(c) zadní vrátka
(d) červi

10. Co znamená zkratka BEC?

a) Certifikát o ekonomice podniku

(b) Porušení zabezpečení e-mailu
c) Příspěvek k obchodnímu úsilí
d) Kybernetický obchodní efekt

11. Termín _____ je dnes veřejností vnímán pejorativně jako jakákoli činnost osoby, která chce získat nelegální přístup do cizího systému nebo osobního počítače.

(a) malware
(b) adware
(c) hacking
(d) podvod

12. Termín _____ je souhrnný pojem zahrnující trestné činy, které porušují práva duševního vlastnictví (velmi často se omezují na autorská práva).

(a) Internetový pirát
(b) Vnímání internetu
(c) Internetové piraně
(d) internetové pirátství

13. Co znamená zkratka DDoS?

(a) Narušené odepření služby
(b) Distribuované odepření služby
c) Rozdělený den služby
(d) Katastrofální slepá ulička služby

14. Co znamená zkratka APT?

a) Pokročilé trvalé hrozby
b) Pokročilá hrozba trestného činu
c) Pokročilé vnímání hrozby
(d) Pokročilá triviální hrozba

Bibliografie

1. *10 nejznámějších hackerských skupin.* [online]. [citováno 15.7.2016]. Dostupné z: https://www.hackread.com/10-most-notorious-hacking-groups/.
2. *7 typů motivace hackerů.* [online]. [citováno 16.8.2015]. Dostupné z: https://blogs.mcafee.com/consumer/family-safety/7-types-of-hacker-motivations/.
3. *7 typů hackerů, které byste měli znát.* [online]. [citováno 16.8.2015]. Dostupné z: https://www.cybrary.it/0p3n/types-of-hackers/.
4. *Životní cyklus pokročilé trvalé hrozby* [online]. [citováno 20. 8. 2016]. Dostupné z: https://upload.wikimedia.org/wikipedia/commons/7/73/Advanced_persistent_threat_lifecycle.jpg.
5. *Pokročilé trvalé hrozby (APT).* [online]. [citováno 20. 8. 2016]. Dostupné z: http://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT.
6. *Pokročilá trvalá hrozba.* [online]. [cit. 20.8.2016]. Dostupné z: https://www.isouvislosti.cz/advanced-persistent-threat.
7. *Pokročilé přetrvávající hrozby: Jak fungují.* [online]. [citováno 10.7.2016]. Dostupné z: https://www.symantec.com/theme.jsp?themeid=apt-infographic-1
8. *Adware.* [online]. [citováno 10.8.2016]. Dostupné z: http://www.mhsaoit.com/computer-networking-previous-assignments/324-lesson-16-h-the-secret-history-of-hacking.
9. *Ransomware pro Android se nyní zaměřuje i na váš Smart TV!* [online]. [citováno 14.8.2016]. Dostupné z: https://thehackernews.com/2016/06/smart-tv-ransomware.html
10. *Rozložení tržních podílů verzí systému Android mezi majiteli chytrých telefonů v květnu 2016.* [online]. [citováno 14.8.2016]. Dostupné z: http://www.statista.com/statistics/271774/share-of-android-platforms-on-mobile-devices-with-android-os/
11. BALIGA, Arati, Liviu IFTODE a Xiaoxin CHEN. Automatizované omezování útoků rootkitů. *Computers& Security*, 2008, roč. 27, č. 7-8, s. 323-334.
12. *Pozor na falešné aplikace pro Android Prisma, které provozují phishing a malware* [online]. [citováno 14.8.2016]. Dostupné z: https://www.hackread.com/fake-android-prisma-app-phishing-malware/
13. *Botnet - historický seznam botnetů.* [online]. [citováno 15.8.2016]. Dostupné z: http://www.liquisearch.com/botnet/historical_list_of_botnets
14. *Botnet.* [citováno 8.7.2016]. Dostupné z: http://research.omicsgroup.org/index.php/Botnet.
15. *Botnet.* [online]. [citováno 15.7.2016]. Dostupné z: https://en.wikipedia.org/wiki/Botnet.
16. *Botnety.* [online]. [citováno 15.7.2016]. Dostupné z: https://www.youtube.com/watch?v=-8FUstzPixU&index=2&list=PLz4vMsOKdWVHb06dLjXS9B9Z-yFbzUWI6.
17. *Boti a botnety - rostoucí hrozba.* [online]. [cit. 11.8.2016]. Dostupné z: https://us.norton.com/botnet/
18. *Buffalo Spammerjde na 7 let za mřížekvůlirozesílánínevyžádanépošty* [online]. [citováno 14.8.2016]. Dostupné z: http://technet.idnes.cz/buffalo-spammer-jde-na-7-let-za-mrize-kvuli-rozesilani-nevyzadane-posty-13i-/tec_reportaze.aspx?c=A040528_28629_tec_aktuality.
19. CARL, Glenn, Richard BROOKS a Rai SURESH. Wavelet-Based Denial-of-Service Detection. *Computers& Security*, 2006, roč. 25, č. 8, s. 600-615.
20. CHOO, Kim-Kwang Raymond. *Online grooming dětí: přehled literatury o zneužívání sociálních sítí k navádění dětí k sexuálním trestným činům* [online]. Canberra: Australian Institute of Criminology, c2009, [cit. 19. 3. 2014]. ISBN 978-1-921532-33-7. Available from:

http://www.aic.gov.au/documents/3/C/1/%7b3C162CF7-94B1-4203-8C57-79F827168DD8%7drpp103.pdf
21. *Boj proti kyberkriminalitě v digitálním věku.* [online]. [citováno 7.5.2016]. Dostupné z: https://www.europol.europa.eu/ec3.
22. *Počítačem vytvořený "miláček" chytá online predátory.* [online]. [citováno 19.8.2016]. Dostupné z: http://www.bbc.com/news/uk-24818769
23. Odsouzený šiřitel spamu napadá zákon státu Va.[online]. [cit. 14.8.2016]. Dostupné z: http://www.usatoday.com/tech/news/techpolicy/2007-09-12-spammer-va_N.htm
24. *Kyberterorismus: jak nebezpečná je hrozba kybernetického chalífátu ISIS?* [online]. [citováno 20.8.2016]. Dostupné z: http://www.govtech.com/blogs/lohrmann-on-cybersecurity/Cyber-Terrorism-How-Dangerous-is-the-ISIS-Cyber-Caliphate-Threat.html
25. *Kyberkriminalita*. [online]. [citováno 1.2.2015]. Dostupné z: http://www.britannica.com/EBchecked/topic/130595/cybercrime/235699/Types-of-cybercrime; et al.
26. *Digi svět digitálního Dooma,* 2008. ISSN 1802-047X. [online]. [citováno 14.8.2016]. Dostupné z: http://www.ddworld.cz/software/windows/jak-se-krade-pomoci-internetu-phishing-v-praxi.html.
27. *Znepokojivé video ISIS ukazuje bojovníky, kteří stínají hlavy čtyřem vězňům, a ozbrojence, který na tržišti obklíčí nakupující.* [online]. [citováno 20.8.2016]. Dostupné z: http://www.mirror.co.uk/news/world-news/disturbing-isis-video-shows-militants-7306017
28. Doplňkový protokol. Dodatkový protokol č. 189 k Úmluvě o počítačové kriminalitě o trestnosti činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189.
29. DODGE, Ronald. C., Curtis CARVE AAARON J. FERGUSON. Phishing pro zvýšení povědomí uživatelů o bezpečnosti. *Computers& Security*, 2007, roč. 26, č. 1, s. 73-80.
30. *Estonsko se vzpamatovává ze silného útoku DDoS.* [online]. [cit. 4. 3. 2010] Dostupné z: http://www.usatoday.com/tech/news/techpolicy/2007-09-12-spammer-va_N.htmhttp://www.computerworld.com/s/article/9019725/Estonia_recovers_from_massive_DDoS_attack.
31. *Exkluzivně: Počítačový virus zasáhl flotilu amerických dronů.* [online]. [cit. 10.7.2016]. Dostupné z: https://www.wired.com/2011/10/virus-hits-drone-fleet/.
32. *Boj proti kyberkriminalitě: kybernetické hlídky a kybernetické vyšetřovací týmy jako posílení strategie EU.* [online]. [cit. 10.7.2016]. Dostupné z: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/08/1827
33. *Klonování Flappy Bird pomáhá zvyšovat míru mobilního malwaru*[online]. [citováno 14.8.2016]. Dostupné z: http://www.mcafee.com/us/security-awareness/articles/flappy-bird-clones.aspx
34. *Ransomware FLocker Mobile přechází na Smart TV* [online]. [citováno 14.8.2016]. Dostupné z: http://blog.trendmicro.com/trendlabs-security-intelligence/flocker-ransomware-crosses-smart-tv/
35. *Francie po utracení milionů zrušila kontroverzní "zákon Hadopi"*[online]. [cit. 15.7.2016]. Dostupné z:https://www.theguardian.com/technology/2013/jul/09/france-hadopi-law-anti-piracy atd.
36. *Lednice zachycená při odesílání spamu v rámci útoku botnetu.* [online]. [citováno 17.5.2016]. Dostupné z: http://www.cnet.com/news/fridge-caught-sending-spam-emails-in-botnet-attack/.
37. GONZÁLES-TALAVÁN, Guillermo. Jednoduchý konfigurovatelný spamový filtr SMTP: Greylists. *Computers&Security*, 2006, roč. 25, č. 3, s. 229-236.
38. GOODMAN, Marc. *Vize kriminality v budoucnosti* [online]. [cit. 13.11.2014]. Dostupné z: https://www.ted.com/talks/marc_goodman_a_vision_of_crimes_in_the_future#t-456071

39. *Společnost Google uvádí, že nejlepší podvody mají 45% úspěšnost.* [online]. [citováno 14.8.2016]. Dostupné z: https://www.engadget.com/2014/11/08/google-says-the-best-phishing-scams-have-a-45-percent-success-r/
40. GREENBERG, Andy. *Hackeři na dálku zabili džíp na dálnici - se mnou uvnitř.* [online]. [citováno 4.5.2016]. Dostupné z: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.
41. GRIFFITHS, Mark. Počítačová kriminalita a hackerství: vážný problém pro policii? *The Police Journal,* 2000, roč. 73, č. 1, s. 18-24.
42. GŘIVNA, Tomáš a Radim POLČÁK. *Kyberkriminalita a právo*. Praha: Auditorium, 2008.
43.
44. HILL, Kašmír. *Tito dva hráči Diabla III ukradli virtuální zbroj a zlato - a byli stíháni na vlastní pěst*. [online]. [citováno 10.8.2015]. Dostupné z: http://fusion.net/story/137157/two-diablo-iii-players-now-have-criminal-records-for-stealing-virtual-items-from-other-players/
45. *Historický seznam botnetů.* [online]. [citováno 15.8.2016]. Dostupné z: http://jpdias.me/botnet-lab//history/historical-list-of-botnets.html.
46. *Historické mapy počítačových sítí.* [Online]. [citováno 10.7.2016]. Dostupné z: https://personalpages.manchester.ac.uk/staff/m.dodge/cybergeography/atlas/historical.html.
47. *Jak APT fungují? Životní cyklus pokročilých perzistentních hrozeb (infografika)* [online]. [citováno 10. 7. 2016]. Dostupné z: https://blogs.sophos.com/2014/04/11/how-do-apts-work-the-lifecycle-of-advanced-persistent-threats-infographic/
48. *Jak používat Wireshark k zachytávání, filtrování a kontrole paketů.* [online]. [citováno 15.7.2016]. Dostupné z: http://www.howtogeek.com/104278/how-to-use-wireshark-to-capture-filter-and-inspect-packets/
49. *Hackerská divize Islámského státu.* [online]. [cit. 20.8.2016]. Dostupné z: https://ent.siteintelgroup.com/index.php?option=com_customproperties&view=search&task=tag&bind_to_category=content:37&tagId=698&Itemid=1355.
50. *Jessica Logan - "The Rest of the Story"* [citováno 8.8.2016]. Dostupné z: http://nobullying.com/jessica-logan/.
51. *Soudci, 69 let, který stahoval dětské porno, hrozí "katastrofální ponížení".* [online]. [citováno 1.9.2009]. Dostupné z: http://news.sciencemag.org/social-sciences/2015/02/facebook-will-soon-be-able-id-you-any-photo
52. *Případ Kevina Mitnicka: 1999* [online]. [citováno 2.11.2011]. Dostupné z: http://www.encyclopedia.com/doc/1G2-3498200381.html
53. KOLOUCH, Jan, Pavel BAŠTA a kol. *Kybernetická bezpečnost*. Praha: CZ.NIC, 2019. ISBN 978-80-88168-31-7.
54. KOLOUCH, Jan. Vývoj phishingových kampaní a kompromitace firemních e-mailů v České republice. In: *Akademický a aplikovaný výzkum ve vojenství a vědě o veřejném řízení*. Budapest: National University of Public Service, 2018, s. 83-100. ISSN 2498-5392.
55. KOLOUCH, Jan. *Kyberkriminalita.* Praha: CZ.NIC, 2016. ISBN 978-80-88168-15-7.
56. KOLOUCH, Jan iAndrera KROPÁČOVÁ. Ransomware. In: ZHUANG, Xiaodong. *Recent Advances in Computer Science: Proceedings of the 19th International Conference on Computers*. B.m.: B.n., 2015, s. 304-307. Recent Advances in Computer Engineering Series, [č. 32]. ISBN 978-1-61804-320-7. ISSN 1790-5109.
57. LEVY, Steven. *Hackers: Heroes of the Computer Revolution* Sebastopol, CA: O'Reilly Media, s. 32-41. ISBN 978-1449388393.
58. LI, Tao, GUAN, Zhihong, WU, Xianyong. Modelování a analýza aktivního šíření červů na základě systémů P2P. *Computers& Security*, 2007, roč. 26, č. 3, s. 213-218.

59. *Malware, chaos a takedown McColo*[online]. [citováno 14.8.2016]. Dostupné z: http://betanews.com/2008/11/13/malware-mayhem-and-the-mccolo-takedown/
60. MARCIÁ-FERNANDÉZ, Gabriel, Jesús E. DÍAZ-VERDEJO a Pedro GARCÍA-TEODORO. Vyhodnocení útoku DoS s nízkou rychlostí proti aplikačním serverům. *Computers& Security*, 2008, roč. 27, č. 7-8, s. 335-354.
61. MELOY, Reid J. *STALKING (OBSESSIONAL FOLLOWING): PŘEHLED NĚKTERÝCH PŘEDBĚŽNÝCH STUDIÍ.* [online]. [citováno 3.10.2015]. Dostupné z: http://forensis.org/PDF/published/1996_StalkingObsessi.pdf.
62. MITNICK, Kevin D. a William L., SIMON. *Přízrak v drátech: moje dobrodružství nejhledanějšího hackera na světě*. New York: Little, Brown & Co, 2012. ISBN 9780316037723.
63. MITNICK, Kevin D. *Umění vniknutí: skutečné příběhy hackerů, narušitelů a podvodníků*. Indianapolis: Wiley, 2006. ISBN 0-471-78266-1.
64. MUELLER, Robert. [Online]. [citováno 3.4.2013]. Dostupné z: https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies.
65. *Nový ransomware šifruje herní soubory.* [online]. [citováno 14.8.2016]. Dostupné z: https://techcrunch.com/2015/03/24/new-ransomware-encrypts-your-game-files/
66. NIGAM, Ruchna. *Časová osa mobilních botnetů.* [online]. [citováno 12.7.2016]. Dostupné z: https://www.botconf.eu/wp-content/uploads/2014/12/2014-2.2-A-Timeline-of-Mobile-Botnets-PAPER.pdf.
67. *OWASP, XSS* [online]. [citováno 15.7.2016]. Dostupné z: https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
68. *Password Sniffer Spy.* [online]. [citováno 18.8.2016]. Dostupné z: http://securityxploded.com/password-sniffer-spy.php.
69. *Zpráva o phishingových aktivitáchTresnds.* [online]. [citováno 14.8.2016]. Dostupné z: https://docs.apwg.org/reports/apwg_trends_report_q1_2016.pdf
70. *Phishing v číslech: statistiky phishingu, které musíte znát v roce 2016* [online]. [citováno 14.8.2016]. Dostupné z: https://blog.barkly.com/phishing-statistics-2016
71. PLETZER, Valentin. Odhalení spywaru. *CHIP*, 2007, č. 10, s. 116-120.
72. PLOHMANN, Daniel, Elmar GERHARDS-PADILLA a Felix LEDER. *Botnety: detekce, měření, dezinfekce a obrana.* ENISA, 2011 [online]. [cit.17.5.2015], s. 14. Dostupné z: https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence.
73. PROSISE, Chris a Kevin MANDIVA. *Incident Response & Computer Forensic, 2. vyd.* Emeryville: McGraw-Hill, 2003.
74. RAK, Roman a Radek KUMMER. Informačníhrozby v letech 2007-2017. *security magazín,* 2007, roč. 14, č. 1, s. 4.
75. *Ransomware.* [online]. [citováno 14.8.2016]. Dostupné z: https://www.trendmicro.com/vinfo/us/security/definition/ransomware.
76. SCHNEIER, Bruce. *Crime: The Internet's Next Big Thing* [online]. [citováno 6.11.2007]. Dostupné z: https://www.schneier.com/crypto-gram/archives/2002/1215.html.
77. SCHNEIER, Bruce. *Internet věcí promění rozsáhlé hackerské útoky v reálné katastrofy* [online]. [citováno 10.8.2016]. Dostupné z: https://motherboard.vice.com/read/the-internet-of-things-will-cause-the-first-ever-large-scale-internet-disaster
78. SCHNEIER, Bruce. *Sedm typů hackerů.* [online]. [cit. 16.8.2015]. Dostupné z: https://www.schneier.com/blog/archives/2011/02/the_seven_types.html.

79. SCHRYEN, Guido. The Impact that Placing Email Addresses on the Internet Has on the Receipt of Spam (Vliv umístění e-mailových adres na internetu na příjem nevyžádané pošty): An Empirical Analysis. *Computers& Security*, 2007, roč. 26, č. 5, s. 361-372.
80. Selfmite - *SMS červ pro Android Selfmite je zpět a je agresivnější než kdy dříve.* [online]. [citováno 14.8.2016]. Dostupné z: http://www.pcworld.com/article/2824672/android-sms-worm-selfmite-returns-more-aggressive-than-ever.html
81. *Statistiky a fakta o spamu.* [online]. [citováno 14.8.2016]. Dostupné z: http://www.spamlaws.com/spam-stats.html
82. *Statistiky spamu*. [online]. [citováno 14.8.2016]. Dostupné z: https://www.spamcop.net/spamstats.shtml.
83. *Stuxnet.* [online]. [cit. 23.7.2016]. Dostupné z: https://cs.wikipedia.org/wiki/Stuxnet.
84. *Časopis o cílených kybernetických útocích.* [online]. [citováno 10.7. 2016]. Dostupné z: https://apt.securelist.com/#secondPage
85. TAYLOR, Harriet. *Jak může být "internet věcí" katastrofální.* [online]. [citováno 17.6.2016]. Dostupné z: http://www.cnbc.com/2016/03/04/how-the-internet-of-things-could-be-fatal.html.
86. *TCP handshake krok za krokem.* [online]. [citováno 18.8.2016]. Dostupné z: http://www.svetsiti.cz/clanek.asp?cid=TCP-handshake-krok-za-krokem-3122000.
87. *Hodnocení hrozeb organizovaného zločinu online (iOCTA) 2014.* [online]. [citováno 10.8.2015]. Dostupné z: https://www.europol.europa.eu/content/internet-organised-crime-threat-assesment-iocta
88. *The Malware Museum @ Internet Archive*. [online]. [citováno 17.5.2016]. Dostupné z: https://labsblog.f-secure.com/2016/02/05/the-malware-museum-internet-archive/.
89. *Svědectví bývalého hackera.* [online]. [citováno 26.9.2008]. Dostupné z: http://www.pbs.org/wgbh/pages/frontline/shows/hackers/whoare/testimony.html
90. *První mobilní malware: jak společnost Kaspersky Lab objevila Cabir*. [online]. [citováno 29.6.2015]. Dostupné z: http://www.kaspersky.com/about/news/virus/2014/The-very-first-mobile-malware-how-Kaspersky-Lab-discovered-Cabir
91. Tinba: *W32. Tinba (Tinybanker).* [Online]. [citováno 15.8.2016]. Dostupné z: https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_w32-tinba-tinybanker.pdf.
92. *Tip měsíce na červenec 2016 - Vyhněte se phishingu*. [online]. [citováno 14.8.2016]. Dostupné z: http://www.intermanager.org/cybersail/tip-of-the-month-july-2016-avoid-getting-hooked-by-phishing/
93. *Hlavní spammer odsouzen na téměř čtyři roky*[online]. [citováno 14.8.2016]. Dostupné z: http://www.pcworld.com/article/148780/spam.html
94. Úmluva o kyberkriminalitě. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
95. *Příručka OSN o prevenci a kontrole počítačové kriminality.* [online]. [citováno 20.8.2016]. Dostupné z: http://216.55.97.163/wp-content/themes/bcb/bdf/int_regulations/un/CompCrims_UN_Guide.pdf
96. *Pozor! Více než 900 milionů telefonů se systémem Android je zranitelných novým útokem "QuadRooter".* [online]. [citováno 10.8.2016]. Dostupné z: https://thehackernews.com/2016/08/hack-android-phone.html
97. *PODÍVEJTE SE: ISIS sundává vězně zaživa, rukojmí vyhazuje do vzduchu pomocí RPG a další zabíjí výbušninami - grafické video.* [online]. [cit. 20.8.2016]. Dostupné z: https://www.zerocensorship.com/uncensored/isis/drowns-prisoners-alive-blows-hostages-up-with-rpg-kills-others-with-explosives-graphic-video-132382

98. WILSON Tracy,V.*Jak funguje phishing*[online]. [cit.14.8.2016]. Dostupné z: http://computer.howstuffworks.com/phishing.htm.
99. Xshqi - *Červ pro Android na čínský Valentýn.* [online]. [citováno 14.8.2016]. Dostupné z: https://securelist.com/blog/virus-watch/65459/android-worm-on-chinese-valentines-day/
100. YAR, Majid. Počítačové hackerství: jen další případ kriminality mladistvých? *The Howard Journal,* 2005, roč. 44, č. 4, s. 387-399.
101. ZETTER, Kim. *Mohou se cestující nabourat do komerčních letadel?* [online]. [citováno 5.5.2016]. Dostupné z: https://www.wired.com/2015/05/possible-passengers-hack-commercial-aircraft/

Modul 4

CSIRT a CERT

1. Úvod

1.1 Shrnutí kurzu

Předmět se zaměřuje na kybernetickou bezpečnost a seznamuje studenty se zásadami vytváření kybernetické bezpečnosti. Pro pochopení celé problematiky je také nutné znát práva a povinnosti bezpečnostních týmů a jejich úkoly, role a procesy. Významná část kurzu se věnuje týmům CERT a CSIRT (struktura, hierarchie) a právnímu zakotvení týmů CERT a CSIRT (práva a povinnosti). Kromě toho by nemělo být opomenuto téma řešení incidentů (IH). Analýza otevřených zdrojů v rámci IH, možnosti přenosu dat a informací jsou také klíčová témata, která tvoří podstatnou část této části kurzu.

1.2 Cíle kurzu

Bezpečnostní incidenty, kybernetické útoky a trestné činy související s informačními a komunikačními technologiemi v reálném i virtuálním světě jsou stále závažnější a jejich důsledky a dopady se zhoršují. Roste potřeba zlepšit obranu proti těmto útokům a zejména zlepšit prostředí a prostředky pro vypátrání pachatele, standardizovat a formalizovat postupy a vzdělávat uživatele v oblasti identifikace, řešení a v ideálním případě i prevence hrozeb a rizikových situací. Za tímto účelem se buduje infrastruktura bezpečnostních týmů, jako jsou CERT a CSIRT. Cílem kurzu je seznámit studenty s těmito bezpečnostními týmy, jejich fungováním, hierarchií, akreditačním procesem, možnostmi sdílení dat a informací atd. Kromě toho se studenti seznámí se systémem řízení bezpečnosti informací. V neposlední řadě zjistí, jaký význam má ochrana dat v kybernetickém prostoru.

1.3 Obsah kurzu

Jednotlivé přednášky seznamují studenty s tématem kybernetické bezpečnosti. Dále jsou studenti seznámeni se zásadami sestavování kybernetické bezpečnosti a bezpečnostního týmu (úkoly, role, procesy atd.) Jedním z klíčových témat jsou CERTy a CSIRTy (struktura, hierarchie) a právní zakotvení CERTů a CSIRTů (práva a povinnosti). Dále studenti studují práva a povinnosti bezpečnostních týmů. Mimořádně důležité je také řešení incidentů (IH), analýza otevřených zdrojů v rámci IH a možnosti přenosu dat a informací, proto je jim věnována poslední část přednášek.

1.4 Cíle učení

1) Úvod do principů vytváření kybernetické bezpečnosti
2) Definování rizik, aktiv a zranitelných míst
3) Porozumění kybernetickým hrozbám a dalším klíčovým pojmům
4) Seznámení se s týmy CERT a CSIRT
5) Definice právního rámce pro CERT/CSIRT

1.5 Potřebné vybavení a materiály

CSIRT a CERT - k dispozici online

Směrnice (EU) 2016/1148 (směrnice NIS)

1.6 Sylabus

Výsledek učení	Student, který úspěšně absolvuje tento modul, bude znát/umět následující.
NOVINKY	
W1	Student získá informace o historickém vývoji bezpečnostních týmů působících v prostředí internetu. Student bude znát role jednotlivých bezpečnostních týmů a právní základ jejich fungování.
DOVEDNOSTI	
U1	Porozumí fungování bezpečnostních týmů, jako jsou CERT a CSIRT, seznámí se s jejich strukturou a vazbami mezi nimi.
U2	Porozumění problematice řešení incidentů.
SOUTĚŽE	
K1	Bude moci působit jako člen bezpečnostního týmu.

Obsah modulu (program přednášek a dalších aktivit)	**Odkaz na výsledky učení**
PŘEDNÁŠKY 1. Kybernetická bezpečnost 2. Zásady pro stanovení kybernetické bezpečnosti 3. Bezpečnostní tým (úkoly, role, procesy atd.) 4. CERT a CSIRT (struktura, hierarchie) 5. Právní pravomoci CERT a CSIRT (práva a povinnosti) 6. Práva a povinnosti bezpečnostních týmů 7. Řešení incidentů (IH) 8. Analýza otevřených zdrojů IH 9. Možnosti přenosu dat a informací WORKSHOPY 1. Vytvoření bezpečnostního týmu	W1, U1, U2, K1

Metody ověřování výsledků učení

Výsledek učení	**Formy kreditních tříd**								
	Ústní zkouška	Písemná zkouška	Částečný písemný úkol	Závěrečný písemný úkol (esej atd.)	Test	Projekt/prezentace	Nahlásit	Činnosti ve třídě	Ostatní ...
NOVINKY									
W1		x			x			x	
DOVEDNOSTI									
U1						x		x	
U2						x		x	
SOUTĚŽE									
K1						x		x	

Zůstatek kreditů ECTS		
Forma pracovní zátěže studentů		Počet hodin
Počet hodin s přímou účastí akademického pracovníka		
1.1	Účast na přednáškách	10
1.2	Účast na seminářích	
1.3	Účast na seminářích	8
1.4	Účast na laboratorních činnostech	
1.5	Účast na projektech	
1.6	Účast na konzultacích (2-3krát za semestr)	
1.7	Účast na konzultacích k projektu	
1.8	Účast na zkouškách/testech	2
1.9	Ostatní ...	
1.10	**Počet hodin strávených za přímé asistence akademických pracovníků (součet 1.1 - 1.9)**	20
1.11	**Počet ECTS kreditů, které student získal v hodinách vyžadujících přímou účast akademického pedagoga)**	1
Individuální práce studentů		
2.1	Individuální studium (včetně e-learningových přednášek)	25
2.2	Individuální příprava na semináře	10
2.3	Individuální příprava na test	
2.4	Individuální příprava na laboratorní výuku	
2.5	Příprava zpráv	
2.6	Realizace samostatně prováděných úkolů (projekty, dokumentace)	
2.7	Příprava na závěrečnou zkoušku/testy semináře	5
2.8	Příprava na závěrečnou zkoušku/testování přednášek	5
2.9	Další	
2.10	**Počet hodin individuální práce (součet 2.1 - 2.9)**	45
2.11	**Počet kreditů ECTS získaných studentem v rámci jednotlivých vzdělávacích aktivit**	1,5
Celková pracovní zátěž (h)		**65**
ECTS kredity za modul		**2,5**

Kritéria pro hodnocení kompetencí studentů
Minimální požadavky na tři skupiny výsledků učení, kterých musí student dosáhnout, aby předmět absolvoval, jsou uvedeny níže v syntetické podobě. Aby Student modul absolvoval, musí být všechny výsledky učení popsané v sylabu pozitivně ověřeny osobou (osobami), která (které) modul vyučuje (vyučují).

W - VĚDOMOSTI
Hodnocení:
Uspokojivý - Student si pamatuje a reprodukuje znalosti, které má v rámci modulu zvládnout.
Dobrý - Žák dodatečně interpretuje jevy / problémy a je schopen vyřešit typický problém.
Velmi dobře -Student je schopen řešit i složité problémy v daném oboru, je schopen syntetizovat, provést komplexní hodnocení, vytvořit práci, která je originální a inspirativní pro ostatní.

U - DOVEDNOSTI
Hodnocení:
uspokojivý - student zná podstatu činností a je schopen pod vedením akademického učitele vykonávat činnosti / řešit problémy související s obsahem modulu.
Dobrý - Student je schopen samostatně provádět činnosti / úkoly / řešit typické problémy související s obsahem modulu.
Velmi dobře - Student si plně osvojil schopnost / dovednost provádět činnosti / úkoly / problémy

stanovené v obsahu modulu, a to i ve složitějších případech.

K - SOCIÁLNÍ KOMPETENCE
Hodnocení:
uspokojivě - student pasivně vstřebává obsah modulu, prokazuje schopnost soustředit se a naslouchat.
Dobrý - Žák se aktivně účastní výuky, vytváří hodnotové soudy podle kritérií přijatých v daném oboru, dokáže aktivně spolupracovat ve skupině.
Velmi dobře - Žák integruje postoje podle navrženého modelu, rozvíjí vlastní systém profesních a společenských hodnot, je schopen převzít odpovědnost za jednání skupiny, včetně vedení.

2. Základní materiály pro učitele

Definice (slovníček pojmů)

Bezpečnost - stav, kdy je ohrožení objektu (nejčastěji národního státu nebo i mezinárodní organizace) a jeho zájmů sníženo na nejnižší možnou míru a objekt je účinně vybaven a ochoten spolupracovat na eliminaci existujících a potenciálních hrozeb."[72]
Bezpečnost - vlastnost objektu nebo subjektu, která určuje míru jeho ochrany před potenciálními škodami a hrozbami."[73]
Bezpečnost - vlastnost položky (např. informačního systému), která je na určité úrovni chráněna proti ztrátě, nebo stav, kdy je chráněna (na určité úrovni) proti ztrátě. Bezpečnost IT zahrnuje ochranu důvěrnosti, integrity a dostupnosti při zpracování, ukládání, distribuci a prezentaci informací. [74]
Kybernetická bezpečnost - je soubor opatření, která jsou přijata k ochraně počítačového systému před neoprávněným přístupem nebo útokem. [75]
Kybernetická bezpečnost je **stav, kdy jsme chráněni před trestným činem nebo neoprávněným použitím elektronických dat**. Kybernetická bezpečnost pak zahrnuje opatření, která je třeba přijmout k dosažení tohoto stavu.[76]
Kybernetická bezpečnost - je "**soubor** právních, organizačních, technických a vzdělávacích **opatření určených k zajištění ochrany kybernetického prostoru.** "[77]
Kybernetická bezpečnost - představuje **soubor** organizačních, politických, právních, technických a vzdělávacích **opatření a nástrojů, jejichž cílem je zajistit bezpečný, chráněný a odolný kybernetický prostor v České republice, a to** jak pro subjekty veřejného a soukromého sektoru, tak pro českou veřejnost obecně." [78]
Kybernetická bezpečnost - týká se bezpečnosti kyberprostoru, přičemž kyberprostorem samotným se rozumí soubor vazeb a vztahů mezi objekty, které jsou přístupné prostřednictvím všeobecné telekomunikační sítě, a vlastní soubor objektů, jejichž rozhraní umožňují jejich dálkové ovládání, dálkový

[72] ZEMAN, Petr a kol. *Česká bezpečnostní terminologie: výklad základních pojmů* [online]. [cit. 2018-07-10]. Dostupné z: http://www.defenceandstrategy.eu/filemanager/files/file.php?file=16048 , s. 13
[73] *POŽÁR, Josef. Informační bezpečnost*. Plzeň: AlešČeněk, 2005, s. 37.
[74] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. Třetí aktualizované vydání. Praha: AFCEA, 2015, s. 23 [online]. [cit. 2018-07-10]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/vykladovy-slovnik-kyberneticke-bezpecnosti---druhe-vydani/.
[75] *Kybernetická bezpečnost.* [online]. [cit. 2018-07-06]. Dostupné z: https://www.merriam-webster.com/dictionary/cybersecurity Překlad autora.
[76] *Kybernetická bezpečnost.* [online]. [cit. 2018-07-06]. Dostupné z: https://en.oxforddictionaries.com/definition/cybersecurity Překlad autora.
[77] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. Třetí aktualizované vydání. Praha: AFCEA, 2015, s. 69 [online]. [cit. 2018-07-10]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/vykladovy-slovnik-kyberneticke-bezpecnosti---druhe-vydani/.
[78] *Národní strategie kybernetické bezpečnosti České republiky 2015-2020 [*online]. [cit. 2018-07-01]. Dostupné z: https://www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf s. 5

přístup k datům nebo zapojení do řídicích činností v kyberprostoru.
Definice kybernetické bezpečnosti podle polského práva je - odolnost informačních systémů vůči činnostem, které narušují důvěrnost, integritu, dostupnost a autenticitu zpracovávaných dat nebo souvisejících služeb nabízených těmito systémy.
Kybernetickou bezpečnost - lze definovat jako: souhrn právních, organizačních, technických a vzdělávacích opatření k zajištění ochrany počítačových systémů a dalších prvků ICT, aplikací, dat a uživatelů,
Kybernetickou bezpečnost lze definovat jako: schopnost počítačových systémů a používaných služeb reagovat na kybernetické hrozby nebo útoky a jejich účinky a plánovat obnovu funkčnosti počítačových systémů a souvisejících služeb.
CIA - zkratky C - **důvěrnost**; **I** - **integrita**; **A - dostupnost.**
Počítačová data - znamenají "**jakékoli vyjádření faktů, informací nebo pojmů ve formě vhodné pro zpracování počítačovým systémem,** včetně programu, který je schopen přimět počítačový systém k provedení **určité** funkce."
Informace "jsou data, která byla zpracována do podoby, jež je pro příjemce užitečná. Každá informace je tedy údaj, ale každý uložený údaj se nemusí nutně stát informací."[79]
Informace - jsou považovány za něco kvalifikovanějšího než data. Data jsou fakta, která se stávají informacemi, když jsou vnímána nebo vyjádřena v kontextu a nesou význam, kterému lidé mohou rozumět.[80]
Přísně tajné - neoprávněné nakládání s informacemi by mohlo způsobit mimořádně vážné škody na státních zájmech.
Tajné - neoprávněné nakládání s informacemi by mohlo způsobit vážnou újmu státním zájmům.
Důvěrné - neoprávněné použití informací by mohlo způsobit běžnou újmu zájmům státu.
Omezené - neoprávněné použití informací by mohlo poškodit zájmy státu.
Chráněné - neoprávněné nakládání s informacemi by mohlo způsobit vážné škody nebo zničení organizace (např. únik strategických informací, zdrojového kódu, bezpečnostních schémat, hesel atd.).
Interní - neoprávněné nakládání s informacemi by mohlo organizaci způsobit škodu (např. únik osobních údajů, smluv atd.).
Citlivé - neoprávněné nakládání s informacemi by mohlo mít pro společnost negativní důsledky (např. nezveřejněné informace o projektech, plánovaných akcích atd.).
Veřejnost - neoprávněné použití informací by nemělo nikoho poškodit a nemělo by mít vliv na veřejnost (např. veřejně dostupné kontakty, prezentace projektů atd.).[81]
TLP je zkratka pro **Traffic Light Protocol**
Přístupnost - je definována jako "vlastnost být dostupný a použitelný na žádost oprávněného subjektu".
IDS - zkratka pro IntrusionDetectionSystém (systém detekce narušení).
IPS - zkratka pro IntrusionPreventionSystém (systém prevence narušení)
Riziko - je "(1) Nebezpečí, možnost škody, ztráty, selhání. (2) Dopad nejistoty na dosažení cílů. (3) Možnost, že hrozba využije zranitelnosti aktiva nebo skupiny aktiv a způsobí organizaci škodu."[82]
Riziko - lze také definovat jako možnost, že se hrozba naplní a využije zranitelnosti aktiva.
Riziko - je definováno jako "**jakákoli rozumně identifikovatelná okolnost nebo událost, která by mohla nepříznivě ovlivnit bezpečnost sítí a informačních systémů**". '
Majetek - cokoli, co má pro osobu, organizaci nebo zemi hodnotu**.**
Majetek - z hlediska občanského práva může být **majetkem hmotná věc (**budova, počítačový systém, síť, energie, zboží atd.) **nebo nehmotná věc** (informace, znalosti, data, programy atd.).

[79] POŽÁR, Josef. *Informační bezpečnost.* Plzeň: AlešČeněk, 2005, s. 25
[80] ŠÁMAL, Pavel a kol. *Kodekskarny II. §§ 140-421. komentář.* Vyd. 2. Praha: C. H. Beck, 2012, s. 2308
[81] Srov. dále: ŠULC, Vladimír. *Kybernetická bezpečnost.* Plzeň: AlešČeněk, 2018. s. 20 a násl.
[82] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. Třetí aktualizované vydání. Praha: AFCEA, 2015. s. 99. Dostupné z: https://nukib.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf.

Aktivum - může být také **vlastnost (např.** dostupnost a funkčnost systému a dat apod.) nebo **pověst** apod. Z hlediska kybernetické bezpečnosti jsou aktivem také **lidé** (uživatelé, správci atd.) a jejich znalosti a zkušenosti.
Podpůrná aktiva - jsou technické zdroje, zaměstnanci a dodavatelé, kteří se podílejí na provozu, vývoji, správě nebo zabezpečení systému ICT.
Primárním aktivem jsou informace nebo služby zpracovávané nebo poskytované systémem ICT.
Zranitelnost - označuje slabé místo v aktivu, softwaru nebo zabezpečení, které je zneužíváno jednou nebo více hrozbami.
Ohrožení - lze nejjednodušeji definovat jako něco, co je schopno narušit normální nebo řádný stav věcí a zasáhnout do práv ostatních. Jedná se o negativní jednání, které může, ale nemusí být uskutečněno
Za hrozbu se považuje "jakýkoli jev, který může způsobit újmu zájmům a hodnotám chráněným státem. Stupeň ohrožení je určen velikostí potenciální újmy a časovou vzdáleností (obvykle vyjádřenou pravděpodobností nebo rizikem) možného uplatnění této hrozby.".[83]
Nebezpečí - je definováno jako "potenciální příčina nezamýšlené události, která by mohla způsobit poškození systému nebo organizace". [84]
Hrozba **informační** bezpečnosti[85] - je definována jako "potenciální příčina nežádoucí události, která by mohla vést k poškození systému a jeho aktiv, jako je zničení, nežádoucí přístup (kompromitace), modifikace dat nebo nedostupnost služeb". [86]
Kybernetická hrozba - je možnost škodlivého pokusu o poškození nebo narušení sítě nebo počítačového systému.[87]
Kybernetickou **hrozbu lze** také definovat jako akci, jejímž cílem je změnit informace, aplikace nebo samotný systém[88] .
Únik informací nastane, když jsou chráněné informace zpřístupněny neoprávněné straně.
Porušení integrity je poškození, změna nebo vymazání dat.
Potlačení služby znamená záměrné zamezení přístupu k informacím, aplikaci nebo systému.[89]
Nezákonné použití je použití informací neoprávněnou osobou nebo neoprávněným způsobem.[90]
"Počítačový bezpečnostní incident" (který lze chápat jako počítačový útok nebo počítačový trestný čin) - nezákonná, neoprávněná, nepřijatelná činnost týkající se počítačového systému nebo sítě.
Bezpečnostní incident - je "**událost, která může způsobit nebo vést k narušení** informačních systémů a technologií a pravidel definovaných k jejich ochraně (bezpečnostní politika)".[91]
Bezpečnostní událost - je **identifikovatelný stav** systému, služby nebo sítě, který **naznačuje možné porušení bezpečnostní politiky nebo selhání bezpečnostních opatření.**
Kybernetický bezpečnostní incident - je **událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb či bezpečnosti a integrity sítí elektronických komunikací.**

[83] *Jeopardy.* [online]. [cit. 2018-07-28]. Dostupné z: http://www.mvcr.cz/clanek/hrozba.aspx.
[84] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. Třetí aktualizované vydání. Praha: AFCEA, 2015. s. 52. Dostupné z: https://nukib.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf.
[85]V tomto případě můžeme zaznamenat problém s překladem některých termínů z angličtiny a naopak. Pokud bychom chtěli důsledně překládat termín Information securitythreat, správný český ekvivalent je např. hrozba informační bezpečnosti; hrozba informační bezpečnosti apod.
[86] Tamtéž, s. 25
[87] *Kybernetická hrozba.* [online]. [cit. 2018-07-06]. Dostupné z: https://en.oxforddictionaries.com/definition/cyberthreat.
[88] Pozměňováním se rozumí také krádež informací, jejich zničení nebo zmaření jejich použití.
[89]Patří mezi ně útoky typu **DoS - Denial of Service**, **DDoS - Distributed Denial of Service** atd. Podrobnější informace naleznete v knize KOLOUCH, Jan. *Kybernetická kriminalita.* Praha: CZ.NIC, 2016, s. 295 a násl.
[90] Například je ohrožen systém založený na poplatcích a jeho služby jsou využívány bez zaplacení služeb.
[91] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. Třetí aktualizované vydání. Praha: AFCEA, 2015. s. 28. Dostupné z: https://nukib.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf.

Bezpečnostní incident - jedna nebo více neúmyslných nebo neočekávaných bezpečnostních událostí, které s vysokou pravděpodobností ohrožují provoz organizace a ohrožují bezpečnost informací.
Počítačový bezpečnostní incident - je porušení nebo bezprostřední hrozba porušení bezpečnostních zásad, zásad přijatelného používání (systému, služby) nebo standardních bezpečnostních postupů."[92]
Kybernetický bezpečnostní incident - je narušení **bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb nebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetického incidentu.**
Kybernetický útok - "útok na IT infrastrukturu s cílem způsobit škodu a získat citlivé nebo strategicky důležité informace. Nejčastěji se používá v souvislosti s politicky nebo vojensky motivovanými útoky."[93]
Kybernetický útok[94] - lze definovat jako **jakoukoli úmyslnou akci útočníka v kyberprostoru, která je zaměřena proti zájmům jiné osoby.**
Kyberkriminalita - může být definována **jako činnost namířená proti počítačovému systému, počítačové síti, datům nebo uživatelům nebo jako činnost, při níž je počítačový systém použit jako nástroj ke spáchání trestného činu.**
CERT - zkratka pro Computer Emergency Response Team
CSIRT - zkratka pro Computer Security Incident Response Team **(**tým pro řešení počítačových bezpečnostních incidentů)
CERT/CSIRT - lze **chápat jako stejný typ týmu - tým, který je zodpovědný za řešení bezpečnostních incidentů a (kybernetických) hrozeb ve své jasně vymezené oblasti působení, z pohledu uživatelů nebo jiných týmů místo, kam se lze obrátit se zjištěným bezpečnostním incidentem, žádostí o spolupráci, výměnu informací, pomoc apod.**
Rozsah působnosti týmu - definuje, za co je tým zodpovědný a jaká je jeho úloha. To samozřejmě závisí na tom, o jaký tým se jedná.
Interní tým - provozuje a odpovídá za určitou síť (např. určitý rozsah IP adres, domén) a je obvykle jmenován provozovatelem sítě.
Koordinační tým - tým, jehož hlavním úkolem je koordinovat řešení bezpečnostních incidentů, nikoli je řešit.
Tým dodavatele - tým zabývající se bezpečnostními incidenty, které se týkají konkrétního produktu (SW).
Národní/vládní tým - zvláštní případy založené na principech prvních dvou zmíněných týmů (interní a koordinační tým), jejich rozsah a úloha závisí na zřizovateli a často i na legislativě konkrétní země.
Back-office - nástroj pro efektivní správu hlášení bezpečnostních incidentů, který umožní sledovat celý životní cyklus hlášení, tj. kdy bylo hlášení odesláno, kým, kdo a v jakých fázích se incidentem zabýval, proč, jakým způsobem byl řešen, kdo koho požádal o spolupráci, jak závažný byl incident a jaké eskalační postupy na něj byly aplikovány atd.
Organizačním základem je již zmíněná "připravenost" k řešení problému, tj. definování základních pravidel týmu tak, aby každý člen týmu znal svou roli, povinnosti a odpovědnost, politiku řešení bezpečnostních incidentů, pravidla komunikace, sdílení a výměny informací, spolupráce atd. Základem v této oblasti je obecně dobře zvládnutý tzv. **incident management.**
FIRST je zkratka pro Fórum pro týmy pro reakci na incidenty a bezpečnost.
TF-CSIRT (Task Force for CSIRT) - je pracovní skupina, která umožňuje týmům spolupracovat na pravidelných dvoudenních schůzkách konaných třikrát ročně (hostitelem této schůzky je obvykle tým CERT/CSIRT).
Školení CSIRT - slouží ke školení nových členů týmů CSIRT/CSIRT nebo těch, kteří se teprve chystají tým

[92] *Průvodce řešením počítačových bezpečnostních incidentů* **[online]. [cit. 2018-02-17]**, s. 6. **Dostupné z:** https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf.

[93] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. Třetí aktualizované vydání. Praha: AFCEA, 2015. s. 71. Dostupné z: https://nukib.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf.

[94] Je nutné odlišit pojem bezpečnostní incident od kybernetického útoku, který představuje porušení bezpečnosti IS/IT a pravidel definovaných k její ochraně (bezpečnostní politika).

CERT/CSIRT založit. Koná se obvykle dvakrát ročně a školiteli jsou zkušení členové renomovaných týmů CERT/CSIRT a další špičkoví bezpečnostní odborníci.
TrustedIntroducer[95] - úřad, jehož hlavním úkolem je budovat důvěru mezi týmy CERT/CSIRT a pomáhat při vytváření nových týmů.
Tým s **uvedeným** statusem o sobě poskytl základní informace, deklaroval ochotu působit jako tým CSIRT a byl komunitou přijat.
Tým s **akreditovaným** statusem deklaruje úroveň praxe, kterou si komunita přeje, a zavazuje se dodržovat společné zásady TI.
Certifikovaný tým pak prokázal svou "úroveň vyspělosti" prostřednictvím certifikačního procesu.
ENISA - Evropská agentura pro bezpečnost sítí a informací.
RIR - zkratka pro regionální internetové registry
Řešení incidentů - proces hlášení a řešení bezpečnostních incidentů.
BotnetFeed - tento nástroj slouží ke zpracování dat ze stažených serverů C&C o koncových stanicích připojených k botnetům. Za účelem identifikace potenciálně infikovaného počítačového systému se správci rozsahu IP předá IP adresa a informace o botnetu, ke kterému je připojen.
IHAP je zkratka pro Incident Handling Automation Project (Projekt automatizace zpracování incidentů).
MDM - zkratka pro Správce škodlivé domény
Indikátory ohrožení - zkratka IoC
Shadowserver - projekt se zaměřuje na průběžné vyhledávání relevantních informací o kybernetických zranitelnostech a výskytu těchto zranitelností na konkrétních IP adresách.

Klíčové citace z online materiálů:

- Slovo **kybernetický** označuje vzájemnou závislost s prvky informačních a komunikačních technologií a kyberprostoru jako takového.
- Mareš definuje bezpečnost jako "*stav, kdy jsou hrozby pro objekt (obvykle národní stát nebo i mezinárodní organizaci) a jeho zájmy sníženy na nejnižší možnou míru a objekt je účinně vybaven a ochoten spolupracovat na eliminaci existujících i potenciálních hrozeb*".[96]
- *Vlastnost položky (např. informačního systému), která je na určité úrovni chráněna proti ztrátě, nebo stav, kdy je chráněna (na určité úrovni) proti ztrátě. Bezpečnost IT zahrnuje ochranu důvěrnosti, integrity a dostupnosti při zpracování, ukládání, distribuci a prezentaci informací.* [97]
- Toto rozšíření okruhu bezpečnosti vyžaduje mimo jiné řešení následujících otázek:
  Čí bezpečnost je ohrožena (mezinárodní organizace, stát, organizace, jednotlivec atd.).

  Jaké hodnoty jsou chráněny (organizace, lidé, data atd.)**?**

  Před čím jsou (měly by být) tyto hodnoty chráněny (fyzické, kybernetické, kombinované útoky atd.)**?**

  Jaké zdroje jsou potřeba k ochraně těchto hodnot? [98]

[95] Delší také **TI**.
[96] ZEMAN, Petr a kol. *Česká bezpečnostní terminologie: výklad základních pojmů* [online]. [cit. 2018-07-10]. Dostupné z: http://www.defenceandstrategy.eu/filemanager/files/file.php?file=16048 . s. 13
[97] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. Třetí aktualizované vydání. Praha: AFCEA, 2015, s. 23 [online]. [cit. 2018-07-10]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/vykladovy-slovnik-kyberneticke-bezpecnosti---druhe-vydani/.
[98] Podrobnější informace lze nalézt například v MAREŠ, Miroslav. *Bezpečnost.* [online]. [cit. 2018-07-10]. Dostupné z: https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=69511.
WAISOVÁ, Šárka. *Bezpečnost: vývoj a koncepční změny.* Plzeň: AlešČeněk, s.r.o., 2005. ISBN 80-86898-21-0.

- Při definování samotné kybernetické bezpečnosti je užitečné vycházet ze zavedených definic. Uvedu několik takových zavedených definic:
    - **Kybernetická bezpečnost** je **soubor opatření, která jsou přijata k ochraně počítačového systému před neoprávněným přístupem nebo útokem**. [99]
    - Oxfordský slovník uvádí, že **kybernetická bezpečnost** je **stav ochrany před kriminálním nebo neoprávněným použitím elektronických dat**. Kybernetická bezpečnost pak zahrnuje opatření, která je třeba přijmout k dosažení tohoto stavu.[100]
    - Podle Jiráska a kol. je **kybernetická bezpečnost** *"**soubor** právních, organizačních, technických a vzdělávacích **opatření určených k zajištění ochrany kybernetického prostoru.** "*[101]
    - Poměrně podobně definuje kybernetickou bezpečnost i Národní strategie kybernetické bezpečnosti České republiky na období 2015-2020, kde se uvádí, že *"kybernetická bezpečnost je **soubor** organizačních, politických, právních, technických a vzdělávacích **opatření a nástrojů směřujících k zajištění bezpečného, chráněného a odolného kybernetického prostoru v České republice,** a to jak pro subjekty veřejného a soukromého sektoru, tak pro českou veřejnost obecně".* [102]
- **Při uplatňování kybernetické bezpečnosti se uplatňují následující zásady, známé také jako kybernetická triáda.**[103]
  Pro účely této monografie budou definovány následující tři triády:

  CIA [**C** - **důvěrnost**; **I** - **integrita**; **A - dostupnost**].

  Prvky kybernetické bezpečnosti (lidé, technologie, procesy).

  Životní cyklus kybernetické bezpečnosti (prevence, detekce, reakce).
- Nejznámější a nejpoužívanější triáda kybernetické bezpečnosti je triáda **CIA,** ale samotné uplatňování této základní triády zásad kybernetické bezpečnosti bez implementace dalších zásad je v současné době nedostatečné pro udržení odpovídající úrovně kybernetické bezpečnosti.
- V literatuře se například poukazuje na použití **Parkerova šekadu**[104] , což je de facto triáda CIA doplněná o další tři prvky: **P/C - Possession/Control**, **A - Authenticity** a **U - Utility**.
- Velmi často je triáda CIA spojována především s informacemi.
  Toto zúžené pojetí vyplývá především ze samotné definice **informační** bezpečnosti, která se zaměřuje na ochranu informací. V souvislosti s touto ochranou není podstatné, na jakém nosiči (papírovém, elektronickém apod.) nebo v jakém systému jsou informace zpracovávány. Bezpečnost informací se pak týká informací v celém jejich životním cyklu.

FRANK, Libor. *Bezpečnostní studie.* [Online]. [cit. 2018-07-10]. Dostupné z: https://moodle.unob.cz/pluginfile.php/35788/mod_page/content/23/Bezpe%C4%8Dnostn%C3%AD%20studia.pdf.

[99] *Kybernetická bezpečnost.* [online]. [cit. 2018-07-06]. Dostupné z: https://www.merriam-webster.com/dictionary/cybersecurity Překlad autora.

[100] *Kybernetická bezpečnost.* [online]. [citováno 2018-07-06]. Dostupné z: https://en.oxforddictionaries.com/definition/cybersecurity Překlad autora.

[101] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. Třetí aktualizované vydání. Praha: AFCEA, 2015, s. 69 [online]. [cit. 2018-07-10]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/vykladovy-slovnik-kyberneticke-bezpecnosti---druhe-vydani/.

[102] *Národní strategie kybernetické bezpečnosti České republiky 2015-2020 [*online]. [cit. 2018-07-01]. Dostupné z: https://www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf s. 5

[103] Viz například HSU, D. Frank a D. MARINUCCI (eds.). *Pokroky v kybernetické bezpečnosti: technologie, operace a zkušenosti*. New York: Fordham University Press, 2013. 272 S. ISBN 978-0-8232-4456-0. s. 41.
KADLECOVÁ, Lucie. *Koncepční a teoretické aspekty kybernetické bezpečnosti.* [online]. [cit. 2018-07-21]. Dostupné z: https://is.muni.cz/el/1423/podzim2015/BSS469/um/Prezentace_FSS_Konceptualni_a_teoreticke_aspekty_KB.pdf.

[104] Podrobnější informace naleznete například v článku *ParkerianHexad*. [Online]. [cit. 2016 8 20]. Dostupné z: https://vputhuseeri.wordpress.com/2009/08/16/149/.

- Bezpečnost informací je také definována řadou norem ISO 27000. Mezi základní normy bezpečnosti informací patří např:
  ISO/IEC 27001:2014 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky
  ISO/IEC 27002:2014 Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření k zajištění bezpečnosti informací
- Podle Úmluvy o počítačové kriminalitě[105] se **počítačovými daty** rozumí *"**jakékoli vyjádření skutečností, informací nebo pojmů ve formě vhodné pro zpracování počítačovým systémem,** včetně programu schopného přimět počítačový systém k provedení **určité** funkce".*
- **Informace** *"jsou data, která byla zpracována do podoby, jež je pro příjemce užitečná. Každá informace je tedy údaj, ale každý uložený údaj se nemusí nutně stát informací."*[106]
- **Informace jsou proto považovány za něco více "kvalifikovaného" než data.** Data jsou fakta, která se stávají informacemi, když jsou vnímána nebo vyjádřena v kontextu a nesou význam, kterému lidé mohou rozumět.[107]
- Pojem důvěrnosti definuje skutečnost, že k informacím, údajům nebo informačním a komunikačním technologiím mají přístup pouze osoby, které jsou k tomu oprávněny.
- Bezpečnostní normy ISO/IEC 27000 stanoví, že:
  "Informace by měly být utajovány s ohledem na jejich hodnotu, právní požadavky, citlivost a kritičnost."
  "Měly by být vypracovány a zavedeny postupy pro označování informací a nakládání s nimi, které jsou v souladu se schématem klasifikace přijatým organizací."
  "Aby se zabránilo neoprávněnému přístupu k informacím nebo jejich zneužití, musí být stanovena pravidla pro nakládání s nimi a jejich uchovávání."
- Příklady některých klasifikačních schémat:
  1. **Utajování informací podle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti**[108] :

- **Přísně tajné** - neoprávněné nakládání s informacemi by mohlo způsobit mimořádně vážné škody na státních zájmech.
- **Tajné** - neoprávněné nakládání s informacemi by mohlo způsobit vážnou újmu státním zájmům.
- **Důvěrné** - neoprávněné nakládání s informacemi by mohlo způsobit běžnou újmu zájmům státu.
- **Omezené -** neoprávněné použití informací by mohlo poškodit zájmy státu.

  2. **Klasifikace informací používaných v komerční sféře**:

- **Chráněné -** neoprávněné nakládání s informacemi by mohlo způsobit vážné škody nebo zničení organizace (např. únik strategických informací, zdrojového kódu, bezpečnostních schémat, hesel atd.).
- **Interní -** neoprávněné nakládání s informacemi by mohlo organizaci způsobit škodu (např. únik osobních údajů, smluv atd.).
- **Citlivé -** neoprávněné nakládání s informacemi by mohlo mít pro společnost negativní důsledky (např. nezveřejněné informace o projektech, plánovaných akcích atd.).

---

[105] čl. 1 písm. b) Úmluvy o počítačové kriminalitě. *Úmluva o kyberkriminalitě.* [online]. [cit. 2016 8 20]. Dostupné z: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804931c0.
[106] POŽÁR, Josef. *Informační bezpečnost.* Plzeň: AlešČeněk, 2005, s. 25
[107] ŠÁMAL, Pavel a kol. *Trestní zákoník II. Komentář k §§ 140-421.* Vyd. 2. Praha: C. H. Beck, 2012, s. 2308
[108] Další podrobnosti naleznete nahttps://www.nbu.cz/cs/pravni-predpisy/zakon-c-412-2005/1122-uplne-zneni-zakona-c-412-2005/.

- **Veřejnost -** neoprávněné použití informací by nemělo nikoho poškodit a nemělo by mít vliv na veřejnost (např. veřejně dostupné kontakty, prezentace projektů atd.).[109]

3. **Protokol semaforu**

- V komunitě kybernetické bezpečnosti historicky existuje potřeba sdílet informace a údaje (obvykle týkající se kybernetických útoků), které jsou citlivé povahy. Z tohoto důvodu vytvořilo Národní koordinační centrum pro bezpečnost infrastruktury[110] na počátku roku 2000 **protokol TrafficLightProtocol(TLP)** .[111]

4. **Posouzení důvěrnosti podle vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, oznamovací povinnosti v oblasti kybernetické bezpečnosti a nakládání s údaji** (vyhláška o kybernetické bezpečnosti).[112]

- Podle Výkladového slovníku kybernetické bezpečnosti[113] **je integrita** definována jako "*vlastnost přesnosti a úplnosti".* **Integrita dat** je ve stejném slovníku dále definována jako *"jistota, že data nebyla změněna". Přeneseně se vztahuje také na platnost, konzistenci a přesnost dat, například databází nebo souborových systémů. Zajišťují ji kontrolní součty, hashovací funkce, samoopravné kódy, redundance, protokolování atd. V kryptografii a informační bezpečnosti obecně se integrita vztahuje k platnosti dat." Integrita* **systému** je tedy *"vlastnost, že systém vykonává svou zamýšlenou funkci nepřetržitě, bez úmyslné nebo náhodné neautomatizované manipulace se systémem".*
- **Integrita tedy znamená, že s informacemi, daty, počítačovými systémy, jejich nastavením** atd. **nemůže manipulovat nikdo jiný než ten, kdo je k tomu oprávněn.**
- Podle Výkladového slovníku kybernetické bezpečnosti[114] **je dostupnost** definována jako "*vlastnost být k dispozici a použitelný na žádost oprávněného subjektu".*
- Dostupnost lze tedy definovat jako záruku možnosti přístupu k informacím, datům nebo počítačovému systému v případě potřeby. Samostatný systém, který zajišťuje integritu a umožňuje přístup k samotnému systému, datům nebo informacím, je k ničemu, pokud nezajišťuje spolehlivý přístup v případě potřeby.[115]
- *"Zničení určitých informací se v informační bezpečnosti označuje jako narušení jejich dostupnosti."*
- Následující tři prvky nebo jejich vzájemné působení umožňují do určité míry vytvořit nebo zavést kybernetickou bezpečnost. Těmito prvky jsou:
    - Lidé,
    - Technologie
    - Procesy.
- Lidé, kteří přicházejí do styku s kybernetickou bezpečností, mohou být vnímáni jako:
  tvůrce (tvůrci) této bezpečnosti (tj. obvykle osoba (osoby), která se snaží prosadit a implementovat různé prvky kybernetické bezpečnosti, ať už pro sebe nebo pro organizaci),

---

[109] Srov. dále: ŠULC, Vladimír. *Kybernetická bezpečnost.* Plzeň: AlešČeněk, 2018. s. 20 a násl.
[110] V současné době Centrum pro ochranu národní infrastruktury - CPNI
[111]Další podrobnosti naleznete např. v části Definice a použití protokolu TLP (TrafficLightProtocol). [Online]. [citováno 2018 Jan 13]. Dostupné z: https://www.us-cert.gov/tlp.
[112] Dále jen nařízení o kybernetické bezpečnosti nebo **VoKB.**
[113] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. Třetí aktualizované vydání. Praha: AFCEA, 2015, s. 58 [online]. [cit. 2018-07-10]. Dostupné z: http://afcea.cz/wp-content/uploads/2015/03/Slovnik_v303.pdf.
[114] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. Třetí aktualizované vydání. Praha: AFCEA, 2015, s. 43 [online]. [cit. 2018-07-10]. Dostupné z: http://afcea.cz/wp-content/uploads/2015/03/Slovnik_v303.pdf.
[115]Viz například EVANS, DONALD, PHILIP, BOND a ARDEN BEMET. *Standardy pro bezpečnostní kategorizaci federálních informací a informačních systémů.* National Institute of Standards and Technology, Computer Security Resource Center. [online]. [citováno 2017 prosinec 10]. Dostupné z: https://csrc.nist.gov/csrc/media/publications/fips/199/final/documents/fips-pub-199-final.pdf.

Příjemci právních předpisů v oblasti kybernetické bezpečnosti (tj. ti, kteří se rozhodli nebo jsou povinni provádět stávající právní předpisy v oblasti kybernetické bezpečnosti),subjekty, které je třeba chránit před kybernetickými útoky,

Subjekty musí být informovány a proškoleny o předpisech a zásadách kybernetické bezpečnosti,

- **Riziko nebo hrozba v kontextu vytváření a udržování kybernetické bezpečnosti**.
- Podle našeho názoru je to důležité pro lidi, kteří používají informační a komunikační technologie a rozhodli se komunikovat v kyberprostoru:
  znát alespoň **základní zásady a pravidla platná pro kybernetickou bezpečnost**,

  rozumí alespoň **základním funkcím počítačových systémů (např.** počítač, notebook, mobilní telefon, chytrá televize atd.), které pro tuto interakci **používají,**

  analyzovat aplikace, které pro tuto interakci **používají,** a pokud se necítí jistí v používání těchto aplikací nebo v porozumění jejich podmínkám, měli by je přestat používat,

  byli vzděláváni v oblasti kybernetické bezpečnosti.
- Technologie obvykle slouží uživatelům k připojení k internetu, sociálním sítím a dalším aplikacím. Je to nástroj, který využívá různé kancelářské balíky k vytváření dokumentů, posílání e-mailů, sledování videí atd. Běžný uživatel zpravidla vnímá a komunikuje s koncovými technologiemi (počítač, tablet, mobilní telefon atd.), které osobně používá, zatímco o další technologické vrstvy, které jsou pro jeho činnost v kyberprostoru nezbytné, se zpravidla nezajímá.
- Pokud jde o technologie, nedílnou součástí ICT organizace by měly být v závislosti na jejích specifikách následující prvky:
  - detekční systémy - systém detekce narušení (**IDS)**/systém prevence narušení (**IPS)**,
  - centrální správa uživatelů a rolí,
  - centralizované řízení klasifikace informací,
  - ochrana proti škodlivému kódu (aplikační firewall, antivirová, antispamová a další řešení),
  - technologie pro zaznamenávání činností jednotlivých komponent ICT, správců a uživatelů (**logovací systém)**,
  - aktivní a offline zálohovací systémy; zálohování důležitých serverů, aplikací a databází (**systém obnovy dat)**,
  - správa zabezpečení sítě (VLAN, DMZ, firewall atd.).
- Procesy jsou činnosti, které je třeba provést, aby lidé mohli využívat technologie a související služby.
- Z hlediska plynutí času lze sledovat následující procesy:
  - řízení aktiv a rizik,
  - definování a kategorizace aktiv,
  - analýza a kategorizace rizik,
  - zavádění informačních a komunikačních technologií a aplikací,
  - správa uživatelů a rolí,
  - autorizace a autentizace,
  - údržba (aktualizace) systémů a služeb,
  - testování bezpečnosti jednotlivých počítačových systémů a služeb,
  - analýzu nápravných opatření,
  - provádění nápravných opatření,

- audit kybernetické bezpečnosti,
- detekce anomálií nebo kybernetických útoků,
- reakce na kybernetické útoky nebo jiné incidenty,
- procesů k zajištění kontinuity,
- školení a cvičení atd.

- Zpětně lze říci, že implementace kybernetické bezpečnosti vyžaduje aplikaci nebo modifikaci jak triády CIA, tak dílčích prvků kybernetické bezpečnosti v průběhu jejich životního cyklu. Zejména prevenci, detekci a reakci na útok. [116]
- Ze zprávy Data BreachInvestigations Report[117] , která analyzuje narušení bezpečnosti vedoucí k ohrožení dat, za rok 2017 vyplývá následující:
- útočník byl
  - **neorganizační osoba - 73 %.**
  - osoba v organizaci - 28 %.
  - **skupina organizovaného zločinu - 50%**
- útočník byl použit k útokům:
  - **hacking - 48 procent.**
  - **malware - 30%**
    - **49 % malwaru bylo** distribuováno a následně nainstalováno útočníkem **prostřednictvím e-mailu.**
  - **sociální inženýrství - 43 %**
  - fyzické napadení - 8%[118]
- obětí jsou organizace působící v:
  - zdravotní péče - 24 %.
  - veřejný sektor (typicky státní správa a místní samospráva atd.) - 14 %.
- motiv útoku:
  - **obohacení - 76 %**
  - získávání dat a informací (špionáž) - 13 %.
- **68 % útoků bylo odhaleno po několika měsících nebo déle.**
- Podle **zprávy Národního úřadu pro kybernetickou a informační bezpečnost** *"**lze v roce 2018 očekávat další nárůst kybernetických hrozeb, zejména** více phishingových útoků nové generace, útoků na tržiště, peněženky a kryptoměnové burzy, bezsouborové varianty ransomwaru, využívání umělé inteligence ke kybernetickým útokům, útoky na data v cloudových řešeních, útoky na internet věcí, průmyslové systémy atd. **Očekává se, že počet státem vlastněných nebo státem sponzorovaných subjektů v kybernetických útocích poroste a že budou pokračovat masivní úniky***

[116] Podrobnější informace naleznete v článku SVOBODA, Ivan. *Řešení kybernetické bezpečnosti.* Přednáška na Akademii CRIF. (23. 9. 2014)
[117] *Zpráva o vyšetřování narušení bezpečnosti dat za rok 2018. 11th Edition.* [Online]. [cit. 2018-07-28]. Dostupné z: http://www.documentwereld.nl/files/2018/Verizon-DBIR_2018-Main_report.pdf.
[118] Jednotlivé útoky obvykle zahrnují kombinaci technik a nástrojů.

osobních údajů, hesel a přístupových údajů. *Proto je nezbytné budovat kybernetickou bezpečnost ICT systémů, které jsou kritické pro fungování státu a jeho kritické infrastruktury."*[119]

- "Kybernetická bezpečnost také pomáhá identifikovat, vyhodnocovat a čelit kybernetickým hrozbám, zmírňovat kybernetická rizika a eliminovat dopady kybernetických útoků, informační kriminality, kyberterorismu a kyberšpionáže při posilování důvěrnosti, integrity a dostupnosti dat, systémů a dalších prvků infrastruktury informačních a komunikačních technologií."
- **Hlavním cílem kybernetické bezpečnosti je chránit prostředí pro realizaci lidských práv na informace."** [120]
- Výkladový slovník kybernetické bezpečnosti definuje riziko jako: "*(1) Nebezpečí, možnost škody, ztráty, selhání. (2) Dopad nejistoty na dosažení cílů. (3) Možnost, že hrozba zneužije zranitelnost zdroje nebo skupiny aktiv a způsobí organizaci škodu."*[121]
- **Riziko lze** také definovat jako **možnost, že se hrozba naplní a využije zranitelnost aktiva**. Podle čl. 4 odst. 9 NIS **je riziko definováno** jako *"**jakákoli rozumně zjistitelná okolnost nebo událost, která by mohla nepříznivě ovlivnit bezpečnost sítí a informačních systémů**". '* V kybernetickém prostoru jsou rizikům vystaveni uživatelé, počítačové systémy a aplikace, které je využívají, a další prvky IKT.
- Pojem **riziko vyjadřuje pravděpodobnost nežádoucí události**. Míra pravděpodobnosti, s jakou tato událost nastane, se vyjadřuje pomocí analýzy rizik. Minimální standardní hodnoty pro metody identifikace, analýzy, hodnocení a vyšetřování rizika jsou uvedeny v normě EN 31010.
- Valášek a kol.[122] uvádějí, že hodnocení rizik je obvykle založeno na třech základních otázkách:
  Co špatného (nežádoucího) se může stát? Co se může pokazit?

  Jaká je možnost/pravděpodobnost, že se tak stane?

  Jak závažné (intenzita, rozsah atd.) mohou být účinky (dopady, důsledky)?
- Pro každé riziko se vypočítá úroveň významnosti rizika, kterou lze vyjádřit následovně:
  Významnost rizika = **dopad** rizika * **pravděpodobnost** výskytu rizika
- **Aktivum je cokoli, co má pro osobu, organizaci nebo zemi hodnotu.**
- Z hlediska občanského práva může být majetek **hmotnou věcí (**budova, počítačový systém, síť, energie, zboží atd.) **nebo nehmotnou věcí** (informace, znalosti, data, programy atd.).
- Aktivem však může být i **vlastnost (např.** dostupnost a funkčnost systému a dat apod.) nebo **pověst** apod. Z hlediska kybernetické bezpečnosti jsou aktivem také **lidé** (uživatelé, správci atd.) a jejich znalosti a zkušenosti.
- V souladu s oddílem 2 písm. f) a g) VoKB se **aktiva dělí** na **vedlejší** a **základní.**
- **Podpůrná aktiva** jsou technické zdroje, zaměstnanci a dodavatelé podílející se na provozu, vývoji, správě nebo zabezpečení systému ICT.
- **Primárním aktivem** jsou informace nebo služby zpracovávané nebo poskytované systémem ICT.

---

[119] *Zpráva o stavu kybernetické bezpečnosti za rok 2017* [online]. [cit. 2018 Jun 29]. Dostupné z: https://nukib.cz/download/Zpravy-KB-vCR/Zprava-stavu-KB-2017-fin.pdf

[120] *Národní strategie kybernetické bezpečnosti České republiky 2015-2020 [*online]. [cit. 2018-07-01]. Dostupné z: https://www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf

[121] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. Třetí aktualizované vydání. Praha: AFCEA, 2015. s. 99. Dostupné z: https://nukib.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf.

[122] VALÁŠEK, Jarmil, František KOVÁŘÍK a kol. *Krizové řízení v nevojenských krizových situacích*. Praha: Ministerstvo vnitra - generální ředitelství Hasičského záchranného sboruČeské republiky, 2008 [online]. [citováno 1. července 2018]. Dostupné z: http://www.hzscr.cz/soubor/modul-c-krizove-rizeni-pri-nevojenskych-krizovych-situacich-pdf.aspx.
ISBN 978-80-86640-93-8 str. 73

- Zranitelností se rozumí slabé místo v aktivu, softwaru nebo zabezpečení, které je zneužíváno jednou nebo více hrozbami.
- Zranitelnost, stejně jako nebezpečí, může být způsobena různými faktory, jako je lidská činnost, technické selhání nebo případně vyšší moc.
- V oblasti kybernetické bezpečnosti se zranitelnosti dělí na:
- **známé** (zveřejněné) **bezpečnostní díry**
    - **záplatované** (**opravené)** - typickým případem jsou zranitelnosti softwaru, pro které již výrobce vydal aktualizaci.
    - **neopravená** - dotčený subjekt (výrobce, správce atd.) o zranitelnosti ví, ale nepostaral se o její opravu.
- **neznámé zranitelnosti**
    - skryté
    - neobjevené
- V příloze 3 vyhlášky o kybernetické bezpečnosti jsou příkladně uvedeny některé zranitelnosti.
  Podle této **vyhlášky jsou zranitelná místa:**
    - nedostatečná údržba informačního a komunikačního systému,
    - zastaralost systému ICT,
    - nedostatečná ochrana vnějšího obvodu,
    - nedostatečné povědomí o zabezpečení mezi uživateli a správci,
    - nesprávné nastavení přístupových práv,
    - nedostatečné postupy pro identifikaci a odhalování nežádoucích bezpečnostních událostí, kybernetických bezpečnostních incidentů a kybernetických bezpečnostních událostí,
    - nedostatečné monitorování uživatelů a správců a neodhalení nevhodného nebo problematického chování,
    - nedostatečná definice bezpečnostních pravidel, nepřesná nebo nejednoznačná definice práv a povinností uživatelů, správců a bezpečnostních rolí,
    - nedostatečná ochrana majetku,
    - nedostatečná bezpečnostní architektura,
    - nedostatečná nezávislá kontrola,
    - včasné neodhalení nesprávného chování zaměstnanců.
- Hrozbu lze nejjednodušeji definovat jako něco, co je schopno narušit normální nebo řádný stav věcí a zasáhnout do práv ostatních. Jedná se o negativní jednání, které může, ale nemusí být realizováno. Pro správnou definici stačí, aby možnost negativního stavu věcí byla bezprostřední a reálná.
- Podle dikce Ministerstva vnitra ČR se za hrozbu považuje "*jakýkoli jev, který má potenciální schopnost poškodit státem chráněné zájmy a hodnoty. Stupeň ohrožení je dán velikostí potenciální škody a časovou vzdáleností (obvykle vyjádřenou pravděpodobností nebo rizikem) možného uplatnění této hrozby.*".[123]

[123] *Jeopardy.* [online]. [cit. 2018-07-28]. Dostupné z: http://www.mvcr.cz/clanek/hrozba.aspx.

- Vlastní pojem hrozba **je** definován jako "*potenciální příčina nechtěné události, která by mohla způsobit poškození systému nebo organizace".* [124]
- S tímto základním pojmem přímo souvisí pojem riziko **informační** bezpečnosti[125] , které je definováno jako "*potenciální příčina nežádoucí události, která by mohla vést k poškození systému a jeho aktiv, jako je zničení, nežádoucí přístup (kompromitace), modifikace dat nebo nedostupnost služeb"*. [126]
- Kromě dvou výše uvedených pojmů autoři ve slovníčku definují pojmy **aktivní hrozba, pasivní hrozba a pokročilá a trvalá hrozba.** [127]
- Oxfordský slovník uvádí, že **kybernetická hrozba je možnost škodlivého pokusu o poškození nebo narušení počítačové sítě nebo systému.**[128] Systémem se v tomto kontextu rozumí počítačový systém.
- Kybernetickou **hrozbu lze** také definovat jako akci, jejímž cílem je změnit informace, aplikace nebo samotný systém[129] .
- Jirovský definuje čtyři skupiny základních hrozeb a charakterizuje jejich vzájemné vztahy:[130]
    - **Únik informací** nastane, když jsou chráněné informace zpřístupněny neoprávněné straně.
    - **Porušení integrity** je poškození, změna nebo vymazání dat.
    - **Potlačení služby** znamená záměrné zamezení přístupu k informacím, aplikaci nebo systému.[131]
    - **Nezákonné použití** je použití informací neoprávněnou osobou nebo neoprávněným způsobem.[132]
- Existuje mnoho klasifikací kybernetických hrozeb, z nichž nejběžnější jsou:

1. Zdroje nebezpečí

a) **Nebezpečí způsobená člověkem.** Pokud je nebezpečí způsobeno člověkem, je třeba se zaměřit také na formu zavinění, která vedla ke vzniku nebezpečí. Z tohoto hlediska lze rozlišovat nebezpečí :

- **Příčinou bylo selhání,**

Mezi záměrně způsobené kybernetické hrozby patří například:

- úmyslné vymazání dat, systémových konfigurací atd,
- fyzické poškození počítačového systému nebo jiné součásti ICT,
- krádež dat a informací,
- kybernetické útoky (malware, DoS, DDoS, phishing, neoprávněný odposlech atd.).[133]

---

[124] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. Třetí aktualizované vydání. Praha: AFCEA, 2015. s. 52. Dostupné z: https://nukib.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf.

[125] V tomto případě můžeme zaznamenat problém s překladem některých termínů z angličtiny a naopak. Pokud bychom chtěli důsledně překládat termín Information securitythreat, správný český ekvivalent je např. hrozba informační bezpečnosti; hrozba informační bezpečnosti apod.

[126] Tamtéž, s. 25

[127] Tamtéž, s. 16, 81 a 87.

[128] *Kybernetická hrozba.* [online]. [citováno 2018-07-06]. Dostupné z: https://en.oxforddictionaries.com/definition/cyberthreat.

[129] Pozměňováním se rozumí také krádež informací, jejich zničení nebo zmaření jejich použití.

[130] Srov. JIROVSKÝ, Václav. *Kyberkriminalita nejen o hackování, crackování, virech a trojských koních bez tajemství.* Praha: Grada Publishing, a. s., 2007. s. 21 a násl.

[131] Patří mezi ně útoky typu **DoS - Denial of Service**, DDoS - **Distributed Denial of Service** atd. Podrobnější informace naleznete v knize KOLOUCH, Jan. *Kybernetická kriminalita.* Praha: CZ.NIC, 2016, s. 295 a násl.

[132] Například je ohrožen systém založený na poplatcích a jeho služby jsou využívány bez zaplacení služeb.

- **způsobené nedbalostí.**

Kybernetická rizika způsobená nedbalostí/neopatrností zahrnují:

- omylem smazaná data,
- fyzické poškození počítačového systému nebo jiného prvku datové komunikace.
- poškození dat, systémů nebo jiných prvků v důsledku neznalosti interních (právních nebo technických) aktů,
- další chyby uživatele.

b) **Technické chyby (např.** chyba softwaru nebo hardwaru).

c) **Vis maior (vyšší moc)**.

Mezi kybernetické hrozby způsobené vyšší mocí patří například:

- neočekávaný výpadek napájení (pokud se nejedná o nebezpečí způsobené lidskou nedbalostí),
- přírodní události (blesky, bouře atd.) nebo katastrofy (povodně, zemětřesení atd.),
- požár (pokud se nejedná o nebezpečí způsobené člověkem).

2. Zdroje působení

a) **Interní hrozby** (zdroj hrozby je uvnitř organizace).

b) **vnější hrozby** (zdroj hrozby je mimo organizaci).[134]

3. Cíle ohrožení

a) Útok triády CIA.

- **Důvěrnost - např.** krádež dat, přístupových údajů a klíčů, počítačového vybavení atd.
- **Integrita** - chyby v databázích, nastavení oprávnění atd.
- **Dostupnost** - např. útoky DoS a DDoS, fyzické útoky na servery a strukturovanou kabeláž, výpadky napájení atd.

b) Útok na prvek kybernetické bezpečnosti.

- **Lidé -** útoky sociálního inženýrství (v reálném světě, ale i v kyberprostoru), phishing, malware, krádeže atd.
- **Technologie -** všechna nebezpečí uvedená v oddíle 1 této klasifikace**.** Typicky mohou nebezpečí působit na:
  - hardware (koncové počítačové systémy, servery, síťové řadiče, IoT atd.).
  - databáze,
  - sítě a síťové infrastruktury,
  - software (operační systém nebo jiné aplikace),
  - informace a data uložená v počítačových systémech.

---

[133] O jednotlivých kybernetických útocích viz například KOLOUCH, Jan. *Kyberkriminalita.* Praha: CZ.NIC, 2016, s. 181 a násl.

[134] Podrobnější informace naleznete například v POŽÁR, Josef. *Vybrané hrozby informační bezpečnosti v organizacích.* [online]. [citováno 6. července 2018]. Dostupné z: https://www.cybersecurity.cz/data/pozar2.pdf.

- **Procesy -** neautorizované testování bezpečnosti nebo funkčnosti procesů nastavených v organizaci apod.

4. **Motivace**

Pokud je hrozba způsobena úmyslným jednáním osoby, je třeba se zabývat motivací hrozby. Analýzou motivace takového jednání lze v rámci procesu reakce na hrozbu vypracovat nápravná opatření, která zabrání tomu, aby tato motivace byla v budoucnu stimulována.
V závislosti na motivaci lze pozorovat:

- ohrožení finančních výhod,
- hrozby s cílem získat konkurenční výhodu,
- hrozby, aby prokázaly své schopnosti,
- odvetné výhrůžky,
- nebezpečí vyplývající z nedodržování předpisů.[135]

5. **Typ nebezpečí**

- sociální inženýrství,
- botnet,
- škodlivý software,
- ransomware,
- spam/podvod,
- podvodné nabídky,
- phishing, pharming, spear phishing, vishing, smishing,
- hackování,
- čichání,
- Útoky DoS, DDoS, DRDoS,
- šíření škodlivého obsahu,
- krádež identity,
- APT (Advanced PersistentThreat),
- kyberterorismus,
- kybernetické vydírání.

V příloze 3 vyhlášky o kybernetické bezpečnosti jsou příkladně uvedeny některé hrozby. **Podle** této **vyhlášky se hrozbou rozumí:**

- porušení bezpečnostních zásad, neoprávněné činnosti, zneužití oprávnění ze strany uživatelů a správců,
- porucha nebo selhání technického vybavení a/nebo softwaru,
- zneužití identity,
- používání softwaru v rozporu s licenčními podmínkami,
- škodlivý kód (např. viry, spyware, trojské koně),
- narušení fyzické bezpečnosti,
- přerušení služeb elektronických komunikací nebo dodávek elektřiny,
- zneužití nebo neoprávněné úpravy údajů,

[135] Před čím se chránit? - Bezpečnostní hrozby, události, incidenty. [Online]. [cit. 2018-07-06]. Dostupné z: https://www.kybez.cz/bezpecnost/pred-cim-chranit

- ztráta, krádež nebo poškození majetku,
- nesplnění smluvního závazku dodavatelem,
- nesprávné chování zaměstnanců,
- zneužití vnitřních zdrojů, sabotáž,
- dlouhodobé přerušení služeb elektronických komunikací, dodávek elektřiny nebo jiných základních služeb,
- nedostatek zaměstnanců s potřebnými znalostmi,
- cílený kybernetický útok s využitím sociálního inženýrství a špionážních technik,
- zneužití vyměnitelných technických paměťových médií,
- zásahy do elektronické komunikace (odposlech, modifikace).

- Prosise a Mandiva charakterizují **"počítačový bezpečnostní incident" (**který lze chápat jako počítačový útok nebo počítačový trestný čin) jako nezákonnou, neoprávněnou a nepřijatelnou akci týkající se počítačového systému nebo sítě. Cílem tohoto jednání může být například krádež osobních údajů, rozesílání spamu nebo jiné obtěžování, zpronevěra, šíření nebo držení dětské pornografie atd.[136]
- Jirásek a kol. definují bezpečnostní ***incident jako "událost, která může způsobit nebo vést k narušení*** *informačních systémů a technologií a pravidel definovaných k jejich ochraně (bezpečnostní politiky)".*[137]
- Definici bezpečnostní události lze nalézt také v bodě 3.5 normy ISO/IEC 27001, kde se uvádí, že takovou událostí je: *"**identifikovatelný stav** systému, služby nebo sítě, který **naznačuje možné porušení bezpečnostní politiky nebo selhání bezpečnostních opatření**. Může to být také jakákoli jiná situace, která předtím nenastala a která může být relevantní pro bezpečnost informací."*
- Podobnou definici lze nalézt v dokumentu NIST 800-61 Computer Security Incident Handling Guide, který uvádí, že bezpečnostní incident je "*událost s negativními důsledky, jako je selhání systému, zahlcení paketů, neoprávněné použití systémových oprávnění, neoprávněný přístup k citlivým údajům nebo spuštění škodlivého kódu, který zničí data*". [138]
- **Kybernetická bezpečnostní událost** je rovněž definována v čl. 7 odst. 1 zákona o kybernetické bezpečnosti jako *"**událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb nebo bezpečnosti a integrity sítí elektronických komunikací**".*
- De facto **se jedná o událost bez reálných negativních důsledků** pro komunikační nebo IT systém, ve skutečnosti jde pouze o hrozbu, která však musí být reálná.

- Vhodná definice **incidentu bezpečnosti informací je uvedena v** normě ISO/IEC 27001. V článku 3.6 této normy je incident bezpečnosti informací definován jako *"jedna nebo více nezamýšlených nebo*

---

[136] PROSISE, Chris a Kevin MANDIVA. *Incident response & computer forensics, 2. vyd.* Emeryville: McGraw-Hill, 2003, s. 13.
Srov. dále CASEY, Eoghan. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, druhé vydání.* London: Academic Press, 2004, s. 9 inast.
[137] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. Třetí aktualizované vydání. Praha: AFCEA, 2015. s. 28. Dostupné z: https://nukib.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf.
[138] *Průvodce řešením počítačových bezpečnostních incidentů* **[online]. [cit. 2018 8 13], s. 6. Dostupné z:** https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf.

neočekávaných bezpečnostních událostí, které s vysokou pravděpodobností ohrožují činnost organizace a ohrožují bezpečnost informací".

- Velmi podobnou definici **počítačového bezpečnostního incidentu** lze nalézt také v dokumentu NIST 800-61 Computer Security Incident Handling Guide, který uvádí, že se jedná o *"porušení nebo bezprostřední hrozbu porušení bezpečnostní politiky, politiky přijatelného používání (systému, služby) nebo standardních bezpečnostních postupů".*[139]
- **Kybernetický bezpečnostní incident** je rovněž definován v § 7 odst. 2 zákona o kybernetické bezpečnosti jako *"**narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb nebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetického incidentu.*** "
- Z dikce zákona je zřejmé, že událost může být způsobena jak úmyslným, tak nedbalostním jednáním člověka, ale také vyšší mocí. Podstatné je, že došlo k **narušení bezpečnosti informací nebo služeb a s nimi spojených systémů IKT.**
- Jirásek a kol. definují kybernetický útok jako "útok na *IT infrastrukturu s cílem způsobit škodu a získat citlivé nebo strategicky důležité informace. Nejčastěji se používá v souvislosti s politicky nebo vojensky motivovanými útoky".*[140]
- **Kybernetický útok**[141] lze definovat jako **jakoukoli úmyslnou akci útočníka v kyberprostoru, která je zaměřena proti zájmům jiné osoby.**
- Při definování obsahu pojmu **kyberkriminalita je důležité si uvědomit,** že s rostoucí možností využití prostředků informačních a komunikačních technologií roste i možnost jejich využití (zneužití) k páchání trestné činnosti. Proto v zásadě neexistuje univerzální, všeobecně přijímaná definice, která by plně vystihovala rozsah a hloubku tohoto pojmu.
- V nejobecnější rovině lze kyberkriminalitu definovat jako **činnost namířenou proti počítačovému systému, počítačové síti, datům nebo uživatelům nebo jako činnost, při níž je počítačový systém využíván jako nástroj ke spáchání trestného činu. Skutečnost, že** počítačová síť nebo kyberprostor je prostředím, v němž se tato činnost odehrává, je pro použití definice kyberkriminality zásadní.

- **CERT** (Computer Emergency Response Team) **aCSIRT** (Computer Security Incident Response Team). Ačkoli každá z těchto zkratek má trochu jiný význam a hlavně trochu jinou historickou genezi, ve skutečnosti lze dnes obě zkratky chápat jako stejný typ týmu - **tým, který je zodpovědný za řešení bezpečnostních incidentů a (kybernetických) hrozeb ve své jasně vymezené oblasti působení, z pohledu uživatelů nebo jiných týmů místo, na které se mohou obrátit se zjištěným bezpečnostním incidentem, požádat o spolupráci, sdílení informací, pomoc apod.**
- Týmy CERT/CSIRT jsou zřizovány na úrovni jednotlivých organizací, a to jak organizací, které zprostředkovávají provoz internetu (poskytovatelé internetových služeb), tak organizací, které využívají internet ke své hlavní činnosti (např. IT společnosti, poskytovatelé obsahu, banky).
- **Primárním úkolem každého týmu CSIRT je reagovat na hrozbu ("reakce") a spolupracovat při řešení incidentů.** Tým CSIRT se obvykle zabývá problémem, který se vyskytne v oblasti jeho odpovědnosti (např. v jeho vlastní síťové infrastruktuře), tj. tam, kde má reálnou moţnost zasáhnout.

---

[139] *Průvodce řešením počítačových bezpečnostních incidentů* **[online]. [cit. 2018-02-17]**, s. 6. **Dostupné z:** https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf.

[140] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. Třetí aktualizované vydání. Praha: AFCEA, 2015. s. 71. Dostupné z: https://nukib.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf.

[141] Je nutné odlišit pojem bezpečnostní incident od kybernetického útoku, který představuje porušení bezpečnosti IS/IT a pravidel definovaných k její ochraně (bezpečnostní politika).

- Nejedná se o nic převratného a prakticky neexistuje; každá větší organizace, poskytovatel internetu nebo služeb má bezpečnostní tým. **Hlavní rozdíl mezi běžným bezpečnostním týmem a CERT/CSIRT spočívá v závazku ke globální bezpečnostní infrastruktuře**, **sdílení informací v rámci** této infrastruktury **a dodržování stanovených formálních postupů**.
- V každé zemi hrají důležitou a **specifickou roli** zastřešující **národní** a **vládní vrcholové týmy,** kterým bude věnována samostatná podkapitola.
- **Základním požadavkem** komunity je**, aby CERT/CSIRT veřejně oznámil své kontaktní údaje a pravidla činnosti:**
    - který je jeho provozovatelem,
    - kteří jsou jejími členy,
    - Jak a kdy lze tým kontaktovat,
    - jaké **služby** nabízí.

  Rozsah (číslo AS[142] , síť, domény, služby), v němž je tým oprávněn jednat a jak, tj. vymezení jeho pravomocí a odpovědnosti. Na základě rozsahu je pak tým kontaktován (např. napadenými) a řeší příslušné problémy (incidenty).
- Termín **řešení bezpečnostních incidentů** může být různě konkrétní v závislosti na konfiguraci týmu a jeho interních politikách - může jít o prostou eliminaci útoku (vyřazení zdroje problému, např. odpojením napadeného počítačového systému od sítě), vypátrání útočníka, rychlé obnovení provozu napadené služby/sítě atd.
- Aby se tým mohl oficiálně nazývat CERT/CSIRT, musí především nabízet službu řešení nebo koordinace řešení bezpečnostních incidentů v rámci své vymezené působnosti, čímž se naplňuje myšlenka "reakce", jak se používá ve zkratkách CERT/CSIRT, tj. musí být schopen *reagovat na* bezpečnostní incident.
- Z "vnějšího" hlediska se tým stává týmem CERT/CSIRT, když je jako takový přijat ostatními existujícími týmy CERT/CSIRT na světě. Cesta k získání statusu týmu CERT/CSIRT není složitá, na začátku cesty stačí jasně deklarovat následující:

1. **Základní kontaktní informace** - název týmu, název organizace, která tým řídí, -e-mailová adresa (adresy) týmu, na kterou lze hlásit bezpečnostní incidenty nebo kontaktovat tým, telefonní číslo (čísla) týmu, adresa kanceláře, jména členů týmu, hodiny, kdy lze tým kontaktovat, atd.
2. **Rozsah působnosti týmu** - definuje, za co je tým zodpovědný a jaká je jeho úloha. To samozřejmě závisí na tom, o jaký tým se jedná. Je možné zřídit týmy zhruba následujících typů:
    - ***Interní*** - provozuje a odpovídá za určitou síť (např. určitý rozsah IP adres, domén) a je obvykle konfigurován provozovatelem sítě,
    - ***Koordinace*** **-** tým, jehož hlavním úkolem je koordinovat řešení bezpečnostních incidentů, nikoli je řešit,
    - ***vendor*** **-** tým zabývající se bezpečnostními incidenty, které se týkají konkrétního produktu (SW),
    - ***národní, vládní*** - zvláštní případy založené na principech prvních dvou zmíněných týmů (interní a koordinační), jejich rozsah a úloha závisí na zřizovateli a často i na legislativě konkrétní země.
3. **Nabízené služby -** CERT/CSIRT musí provozovat minimálně službu reakce na bezpečnostní incidenty.

- **Organizačním základem je** již zmíněná "připravenost" k řešení problému, tj. definování základních pravidel týmu tak, aby každý člen týmu znal svou roli, povinnosti a odpovědnost, politiku řešení

[142] **AS** - autonomní systém. Autonomní systém je soubor IP sítí a směrovačů pod společnou technickou správou, který představuje společnou směrovací politiku vůči internetu.

bezpečnostních incidentů, pravidla komunikace, sdílení a výměny informací, spolupráce atd. Základem v této oblasti je obecně dobře zvládnutý tzv. ***incident management.***

- CERT/CSIRT jsou zřizovány na dobrovolné bázi a mají zájem na efektivní vzájemné komunikaci, sdílení relevantních informací a znalostí a spolupráci. Z tohoto důvodu se týmy sdružují v mezinárodních organizacích. V současné době jsou nejznámějšími a nejaktivnějšími organizacemi, které se touto problematikou zabývají a vytvářejí vhodné prostředí pro dosažení výše uvedených cílů, mezinárodní organizace **GÉANT**[143] a **FIRST** (Forum for IncidentResponse and Security Teams)[144] .
- Evropská organizace GÉANT pořádá několik aktivit, kterých se v případě zájmu mohou účastnit globální CERT/CSIRT:

  TF-CSIRT (Task Force for CSIRT) je pracovní skupina, která umožňuje týmům spolupracovat na pravidelných dvoudenních schůzkách konaných třikrát ročně (hostitelem této schůzky je obvykle tým CERT/CSIRT). Více informací naleznete na adrese: https://tf-csirt.org/.

  Školení CSIRT - slouží ke školení nových členů týmů CSIRT/CSIRT nebo těch, kteří se teprve chystají tým CERT/CSIRT založit. Koná se obvykle dvakrát ročně a školiteli jsou zkušení členové renomovaných týmů CERT/CSIRT a další špičkoví bezpečnostní odborníci. Více informací naleznete na adrese: https://tf-csirt.org/transits/.

  TrustedIntroducer[145] - úřad, jehož hlavním úkolem je budovat důvěru mezi týmy CERT/CSIRT a pomáhat při vytváření nových týmů. Více informací naleznete na adrese: https://www.trusted-introducer.org/.

- Mezi stávajícími týmy musí být také alespoň dva týmy (tzv. sponzoři), které budou nový tým podporovat, a žádný ze stávajících týmů nemůže mít proti přijetí nového týmu námitky. Pokud vše proběhne v pořádku, informace o novém týmu jsou vedeny na seznamu vedeném kanceláří TI (a některé z nich jsou zveřejněny), tým získá status týmu ***uvedeného na seznamu*** a komunita nového člena přivítá.
- V případě FIRST je vstupní procedura velmi podobná, ale končí ***členstvím,*** nikoli statusem.
- S TrustedIntroducer je možné získat další, důležitější statusy, a to ***akreditovaný*** a ***certifikovaný***. Rozdíly jsou následující:

  Tým, který byl zařazen do seznamu, o sobě ***poskytl*** základní informace, deklaroval ochotu chovat se jako tým CSIRT a byl komunitou přijat.

  Tým s ***akreditovaným*** statusem deklaruje úroveň praxe, kterou si komunita přeje, a zavazuje se dodržovat společné zásady TI.

  Certifikovaný tým pak prokázal svou "úroveň vyspělosti" prostřednictvím certifikačního procesu.
- ***Akreditace*** nebo ***certifikace týmu*** vyžaduje trvalé úsilí o udržení statusu týmu. Součástí tohoto úsilí je povinnost aktualizovat informace o týmu v seznamu TI. Pokud tak nebudete činit delší dobu, může to vést ke ztrátě statusu týmu a v nejhorším případě k vyloučení z komunity.

- Další organizací působící v oblasti bezpečnosti je **ENISA** (Evropská agentura pro bezpečnost sítí a informací, http://www.enisa.europa.eu/). Úzce spolupracuje s členskými státy EU a soukromým sektorem a zahrnuje celou řadu činností, včetně celoevropských cvičení v oblasti kybernetické bezpečnosti, vypracovávání národních strategií kybernetické bezpečnosti, spolupráce a budování kapacit mezi skupinami CERT/CSIRT, řešení otázek ochrany osobních údajů a práce na vývoji a provádění právních předpisů v oblasti bezpečnosti síťových informací (NIS).

[143] Sdružení vzniklo sloučením sdružení TERENA (Trans-EuropeanResearch and Education Networking Association) a DANTE.

[144] Další informace o soutěži FIRST najdete na adrese: https://www.first.org

[145] Delší také **TI**.

- **Týmy CERT/CSIRT nemají žádnou oficiální hierarchii,** která by jeden tým nadřazovala druhému. **Všechny týmy jsou si z** hlediska fungování, komunikace, spolupráce a sdílení informací **rovny** a nejsou v těchto oblastech omezovány.
- Ve světě týmů CERT/CSIRT je klíčová **ochota sdílet důležité informace o** incidentech a hrozbách. K tomu je nezbytné, aby si týmy navzájem důvěřovaly a aby uživatelé důvěřovali svým týmům.

- **Národní tým CERT/CSIRT** funguje jako **poslední *instance, na kterou* je možné se obrátit** s žádostí o **pomoc a zásah**. Jeho účelem (v rámci země nebo regionu, kde působí) je působit jako prostředník mezi napadenou stranou a iniciátorem problému a usnadnit jeho úspěšné vyřešení.

- Týmy zemí (obvykle) nemají kontrolu nad fyzickou infrastrukturou, takže nemají (na rozdíl od interních/institucionálních týmů) možnost přímo zasahovat. Jejich úlohou je zprostředkovávat kontakty nebo koordinovat (odtud typ **koordinační** tým) činnost různých aktérů, pokud je problém větší a vyžaduje spolupráci více aktérů.

- Národní CERT/CSIRT má obvykle ve svých povinnostech **vzdělávání a spolupráci.** To zahrnuje jak vzdělávání veřejnosti, tak práci v rámci internetové infrastruktury. Cílem je podporovat zakládání dalších CERT/CSIRT v zemi, jejich uvedení na mezinárodní scénu a podpora zavádění standardních postupů a praktik. To vše výrazně zvyšuje transparentnost prostředí a dává napadeným šanci na účinnou nápravu.
- **Vládní CERT/CSIRT** se obvykle zaměřují na státní a místní orgány a na řešení incidentů, které ohrožují bezpečnost státu a jeho služeb. Vládní CERT/CSIRT může mít podobu interního týmu se schopností přímo zasáhnout v případě problému. Jeho existence je obvykle podpořena legislativou.
- **Proces hlášení a řešení bezpečnostních incidentů** (nebo vlastně "na koho se mám obrátit, abych nahlásil nebo vyřešil bezpečnostní incident") **lze posuzovat ze dvou hledisek.** Z pohledu **techniků** (správců sítě a služeb, členů bezpečnostního týmu) a z pohledu **uživatelů.**

- Pro **techniky** (správce sítí a služeb, členy bezpečnostních týmů) je odpověď na otázku "na koho se mám vlastně obrátit, aby přijal opatření" zcela zřejmá, ale vyplývá ze zkušeností a především z velmi dobré znalosti internetového prostředí a jeho základních principů, stejně jako z toho, kde najít kontaktní informace o různých existujících sítích, službách, doménách atd.
- Regionální internetové registry (**RIR)** uchovávají a sdílejí informace o tom, komu byl přidělen blok IP adres. Svět je rozdělen do regionů a každý RIR (v současnosti RIPE, ARIN, APNIC, LACNIC, AFRINIC) přiděluje IP adresy pro svůj region. Region Evropy, Středního východu a části Asie spravuje RIPE NCC (https://www.ripe.net/).

- Proces hlášení a řešení bezpečnostních incidentů (odborně incident ***handling)*** není striktní, naopak, hodně záleží na zkušenostech a někdy i kreativitě osoby, která tento proces provádí. Výměna informací mezi týmy je obvykle rychlá a efektivní, i když ani to často nezaručuje rychlé vyřešení, protože celková infrastruktura je na to stále ještě poměrně "řídká" a bohužel je třeba říci, že úroveň týmů je různá.
- **Optimální stav infrastruktury by byl, kdyby každá IP adresa byla v dosahu oficiálního CSIRT.** V této situaci je však infrastruktura týmů CERT/CSIRT na hony vzdálená.
- **Z pohledu běžného uživatele** je situace velmi nepřehledná a v podstatě matoucí. Co má tedy uživatel v případě bezpečnostního incidentu dělat a na koho se má obrátit? Těžko lze po uživateli požadovat, aby se dozvěděl o CERT/CSIRT, našel ten správný, prostudoval jeho zásady hlášení bezpečnostních incidentů a podnikl příslušné kroky.

- V první řadě by **se** uživatelé měli **obrátit na svého správce sítě nebo služby** (pokud ho mají) nebo na svého poskytovatele připojení, tj. **helpdesk poskytovatele internetových služeb nebo jeho uživatelskou podporu**. Na straně poskytovatele internetového připojení by mělo existovat jasně popsané kontaktní místo, na které se uživatelé mohou a měli by se obrátit, pokud se stanou terčem útoku, zjistí bezpečnostní incident nebo mají pocit, že něco není v pořádku.
- **Mezi týmem země a vládním týmem probíhá velmi úzká spolupráce** a výměna informací a relevantních údajů, a tak se nahlášený problém předává k řešení jednomu týmu nebo se přímo pracuje na jeho řešení.
- **Obecně by však bylo žádoucí, aby správci sítí a služeb a členové bezpečnostních týmů ovládali a uplatňovali zásady procesu řešení incidentů a maximalizovali komunikaci přímo (**nikoli prostřednictvím týmů vyšší úrovně). Díky tomu je proces řešení incidentů rychlý a efektivní; další mezikroky mohou přinést zpoždění a bohužel i narušení. Ale jak již bylo zmíněno, záleží na závažnosti situace a řešeného problému

- **CERT/CSIRT a jejich infrastruktura nejsou obecně komplexní a nepředstavují bezpečnost "v kostce"**.

- Dne 6. července 2016 přijal Evropský parlament směrnici Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních pro vysokou společnou úroveň bezpečnosti sítí a informačních systémů v Unii (směrnice o bezpečnosti sítí a informací).

- Na základě zákona o kybernetické **bezpečnosti jsou v České republice povinně zřízeny dva týmy** CERT/CSIRT**: národní a vládní**. Každý z těchto týmů má přesně vymezená zákonná práva a povinnosti (§ 17 a násl. zákona o CERT).
- Směrnice o bezpečnosti sítí a informací stanoví právní opatření ke zvýšení celkové úrovně kybernetické bezpečnosti v EU tím, že zajistí:
    - připravenost členských států tím, že od nich vyžaduje, aby byly dostatečně vybaveny. Například v týmu pro reakci na počítačové bezpečnostní incidenty (CSIRT) a v příslušném vnitrostátním orgánu NIS,
    - spolupráce mezi všemi členskými státy prostřednictvím vytvoření skupiny pro spolupráci, která bude podporovat a usnadňovat strategickou spolupráci a výměnu informací mezi členskými státy.
    - kulturu bezpečnosti v odvětvích, která jsou klíčová pro naše hospodářství a společnost a která jsou do značné míry závislá na IKT, jako je energetika, doprava, vodní hospodářství, bankovnictví, infrastruktura finančních trhů, zdravotnictví a digitální infrastruktura.
- Členské státy zaujaly k provádění NIS různé přístupy.

3. Během výuky

<u>Několik nápadů na aktivity:</u>

WORKSHOPY

1. analyzovat potřebu bezpečnostního týmu v organizaci.
2. Definice jednotlivých aktiv a SWOT analýza ve vztahu k nim.
3. Vytvoření a začlenění bezpečnostního týmu do organizace - přijetí pravidel a zásad.
4. Simulace kybernetického incidentu nebo události namířené proti organizaci.
5. Řízení incidentů.
6. Analýza přijatých opatření.
7. Sdílení informací s ostatními.

KONTROLNÍ OTÁZKY

1.

- Co je triáda CIA?
- Jak lze definovat kybernetickou bezpečnost?
- Jaké jsou prvky kybernetické bezpečnosti?
- Co se rozumí aktivy?
- Jak lze definovat zranitelnost?

2.

- Co je to tým CSIRT/CERT?
- Jak se tým CSIRT/CERT vytváří a zakládá?
- Na co se zaměřuje národní tým CSIRT?
- Na co se zaměřuje vládní tým CSIRT?
- Jaké jsou základní požadavky komunity na tým CSIRT/CERT?

3.

- Existuje hierarchie mezi týmy CSIRT/CERT?
- Jak je definována působnost týmu CSIRT/CERT?
- Kdo je vládní tým CSIRT/CERT?
- Kdo je národní tým CSIRT/CERT?
- Jaké jsou role a odpovědnosti ostatních týmů CSIRT/CERT?
- Jak jsou ve vaší zemi sestaveny týmy CSIRT/CERT?

Práce ve dvojicích/skupinách

- **Dvojice - miniprojekt**
  Studenti si ve dvojicích vyberou jedno z probíraných témat. Zapíší své závěry a představí je ostatním. Po prezentaci si ostatní studenti připraví doplňující otázky pro prezentující skupinu.

- **Mapa myšlenek**
  Studenti si ve dvojicích vyberou jedno z probíraných témat a vytvoří myšlenkovou mapu, kterou pak v krátké prezentaci popíší ostatním studentům.

- **Klíčová slova**
  Studenti ve dvojicích samostatně vyberou klíčová slova ze slovníčku.

Definice těchto slov napíší na proužky papíru. Proužky otočí prázdnou stranou nahoru. Jeden student si vybere proužek, přečte definici a druhý student hledá odpovídající klíčové slovo.
nebo
Studenti si na papír napíší několik klíčových slov ze slovníčku. Kartičky otočí prázdnou stranou nahoru. Jeden student si vezme první kartičku a řekne, co dané slovo znamená. Druhý student klíčové slovo hádá.

- 10 klíčových slov

  Studenti si vyberou 10 klíčových slov souvisejících s vybraným tématem. Těchto 10 klíčových slov předají ostatním dvojicím. Dvojice napíší text, který musí obsahovat všechna klíčová slova. Jedna věta může obsahovat pouze jedno klíčové slovo. Text se tedy skládá minimálně z 10 vět.

- Panelová diskuse

  Studenti si vyberou 3 řečníky. Každý řečník si vybere jedno téma, o kterém bude diskutovat. Ostatní studenti kladou otázky k tématům. Každý mluvčí může použít typ odpovědi -PRAVDA X NEPRAVDA. Za každou pravdivou odpověď získá student bod, např. znamená GDPR General Data Protection Regulation? - PRAVDA X NEPRAVDA.

4. Internetové zdroje

Viz bibliografie níže

5. Další otázky/testy

VYBERTE SPRÁVNOU ODPOVĚĎ:
(Správná odpověď byla zvýrazněna)

1. _____ je soubor opatření přijatých k ochraně počítačového systému před neoprávněným přístupem nebo útokem.

   a) Cybersafe
   (b) Bezpečnost v kyberprostoru

c) Kybernetická bezpečnost
d) Cybersecure

2. Mezi prvky kybernetické bezpečnosti patří: _____

(a) lidé, technologie, procesy

(b) realita, software, hardware

(c) dodavatelé, virtualita, postupy

(d) uživatelé, technologie, problémy

3. _____ označuje situaci, kdy k informacím, datům nebo informačním a komunikačním technologiím mají přístup pouze ti, kteří jsou k tomu oprávněni.

(a) Důvěryhodnost
b) Realita
(c) Autentičnost
(d) Důvěrnost

4. Pro každé riziko se vypočítá stupeň významnosti rizika, který lze vyjádřit následovně:
a) Významnost rizika = dopad rizika * pravděpodobnost výskytu rizika
(b) Významnost rizika = rozsah rizika * pravděpodobnost rizika.
c) Významnost rizika = dopad rizika * možnost výskytu rizika
d) Významnost rizika = Rizikové problémy * Pravděpodobnost výskytu rizika

5. _____ jsou technické prostředky, zaměstnanci a dodavatelé podílející se na provozu, vývoji, správě nebo zabezpečení systému ICT.

(a) Podkladová aktiva
(b) Běžná aktiva
(c) příjmy
(d) Vedlejší aktiva

6. _____ označuje slabinu v prostředku, softwaru nebo zabezpečení, kterou využívá jedna nebo více hrozeb.

a) Křehkost
(b) Zranitelnost
c) Slabost
(d) Pochybnost

7. _____ je možnost škodlivého pokusu o poškození nebo narušení sítě nebo počítačového systému.

a) Kybernetická hrozba
(b) Kyberkultura
c) Kybernetická energie
d) Kyberkriminalita

8. **Co znamená** zkratka **CSIRT**?

(a) Tým pro řešení počítačových havarijních situací
(b) Reakce týmu na počítačové bezpečnostní incidenty
(c) Tým pro řešení počítačových havarijních situací
(d) Tým pro reakci na počítačové bezpečnostní incidenty

9. Týmy CERT/CSIRT nemají žádnou oficiální hierarchii, která by jeden tým nadřazovala druhému. Všechny týmy jsou _____, pokud jde o fungování, komunikaci, spolupráci a sdílení informací, a nejsou v těchto oblastech omezeny.

(a) různé
(b) stabilní
(c) stejný
(d) nespecifikované

10. Členské státy přijaly k provádění NIS přístupy _____.

(a) stejný
(b) totožný
(c) společné
(d) různé

11. Co znamená CIS?

a) Péče, vliv, dostupnost
(b) Důvěrnost, integrita, dostupnost
c) Spolupráce, integrita, dostupnost
d) dopad, důvěryhodnost, dostupnost

12. Rozdíl mezi běžným bezpečnostním týmem a CERT/CSIRT spočívá především v zapojení do infrastruktury _____**,** výměně informací v rámci této infrastruktury a dodržování stanovených formálních postupů**.**

(a) národní bezpečnost
(b) globální nepokoje
(c) globální hrozba
(d) globální bezpečnost

13. Co znamená zkratka ENISA?

(a) Evropská agentura pro bezpečnost sítí a informací.
b) Evropská agentura pro síťovou a informační bezpečnost (European Netsurfers and Information Security Agency)
(c) Evropská agentura pro jednání a bezpečnost informací
(d) Evropská agentura pro národní bezpečnost a informace

14. _____ - tým, který se zabývá řešením bezpečnostních incidentů, jež se týkají konkrétního produktu.

a) Interní
b) Vláda
(c) Prodejce
(d) Koordinace

Bibliografie

1. *Zpráva o vyšetřování narušení bezpečnosti dat za rok 2018. 11th Edition.* [Online]. [cit. 2018-07-28]. Dostupné z: http://www.documentwereld.nl/files/2018/Verizon-DBIR_2018-Main_report.pdf.
2. *Analýza rizik [*online]. [citováno 2018-07-01]. Dostupné z: https://www.vlastnicesta.cz/metody/analyza-rizik-risk/.
3. ANDRESS, Jason. *Základy informační bezpečnosti*. 2. vydání. Syngress. 9780128007440
4. CASEY, Eoghan. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, Second Edition.* London: Academic Press, 2004, s. 9 a násl.
5. *Metodiky CIA.* [online]. [cit. 2018-07-10]. Dostupné z: https://en.wikipedia.org/wiki/Information_security#/media/File:CIAJMK1209.png.
6. *Průvodce řešením počítačových bezpečnostních incidentů* **[online]. [cit. 2018 8 13]**, s. 6. **Dostupné z:** https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf.
7. *Kybernetická bezpečnost.* [online]. [cit. 2018-07-06]. Dostupné z: https://en.oxforddictionaries.com/definition/cybersecurity Překlad autora.
8. *Kybernetická bezpečnost.* [online]. [cit. 2018-07-06]. Dostupné z: https://www.merriam-webster.com/dictionary/cybersecurity Překlad autora.
9. *Kybernetická hrozba.* [online]. [cit. 2018-07-06]. Dostupné z: https://en.oxforddictionaries.com/definition/cyberthreat.
10. *Definice kybernetické bezpečnosti - mezery a překryvy ve standardizaci*. [online]. [cit. 2017 12 10]. Dostupné z: https://www.enisa.europa.eu/publications/definition-of-cybersecurity s. 30
11. *Model hodnocení vyspělosti CSIRT agentury ENISA* [online], 2019. VERZE 2.0. Atény, Řecko: Agentura Evropské unie pro bezpečnost sítí a informací (ENISA) [cit. 2021-03-16]. ISBN 978-92-9204-292-9. Dostupné z: https://www.enisa.europa.eu/publications/study-on-csirt-maturity/at_download/fullReport, s. 6.
12. EVANS, DONALD, PHILIP, BOND a ARDEN BEMET. *Standardy pro kategorizaci bezpečnosti federálních informací a informačních systémů*. NationalInstitute of Standards and Technology, Computer Security Resource Center. [online]. [citováno 2017 prosinec 10]. Dostupné z: https://csrc.nist.gov/csrc/media/publications/fips/199/final/documents/fips-pub-199-final.pdf.
13. FRANK, Libor. *Bezpečnostní studie.* [Online]. [cit. 2018-07-10]. Dostupné z: https://moodle.unob.cz/pluginfile.php/35788/mod_page/content/23/Bezpe%C4%8Dnostn%C3%AD%20studia.pdf.
14. FRUHLINGER, Josh. *Co je Stuxnet, kdo ho vytvořil a jak funguje?* [online]. [citováno 2018-07-01]. Dostupné z: https://www.csoonline.com/article/3218104/malware/what-is-stuxnet-who-created-it-and-how-does-it-work.html.
15. HENDERSON, Anthony. *Triáda CIA: důvěrnost, integrita, dostupnost.* [Online]. [cit. 2018]. Dostupné z: http://panmore.com/the-cia-triad-confidentiality-integrity-availability.
16. *Jeopardy.* [online]. [cit. 2018-07-28]. Dostupné z: http://www.mvcr.cz/clanek/hrozba.aspx.
17. HSU, D. Frank a D. MARINUCCI (eds.). *Pokroky v kybernetické bezpečnosti: technologie, operace a zkušenosti*. New York: Fordham University Press, 2013. 272 S. ISBN 978-0-8232-4456-0. S. 41.
18. JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. Třetí aktualizované vydání. Praha: AFCEA, 2015, s. 23 [online]. [cit. 2018-07-10]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/vykladovy-slovnik-kyberneticke-bezpecnosti---druhe-vydani/.
19. JIROVSKÝ, Václav. *Kyberkriminalita nejen o hackování, crackování, virech a trojských koních bez tajemství.* Praha: Grada Publishing, a. s., 2007. s. 21 a násl.

20. KADLECOVÁ, Lucie. *Koncepční a teoretické aspekty kybernetické bezpečnosti.* [online]. [cit. 2018-07-21]. Dostupné z: https://is.muni.cz/el/1423/podzim2015/BSS469/um/Prezentace_FSS_Konceptualni_a_teoreticke_aspekty_KB.pdf.
21. KOLOUCH, Jan. *Kyberkriminalita.* Praha: CZ.NIC, 2016.
22. *Kybernetická bezpečnost: co s tím?* [online]. [cit. 2018 Jun 29]. Dostupné z: http://www.businessinfo.cz/cs/clanky/kyberneticka-bezpecnost-co-s-tim-84467.html
23. *Macronův volební štáb napadli hackeři, tvrdí japonská antivirová firma.* [online]. [cit. 2017 Jun 29]. Dostupné z:http://zpravy.idnes.cz/macron-utok-hackeri-trend-micro-d3b-/zahranicni.aspx?c=A170425_071554_zahranicni_san
24. MAREŠ, Miroslav. *Bezpečnost.* [Online]. [cit. 2018-07-10]. Dostupné z: https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=69511.
25. MATUROVÁ, Jana a Miroslav VALTA. *Prevence rizik - kontroly stavu technických zařízení.* [Online]. [citováno 1. července 2018]. Dostupné z: https://www.bozpinfo.cz/prevence-rizik-provadeni-kontrol-technickeho-stavu-technickych-zarizeni.
26. *Národní strategie kybernetické bezpečnosti České republiky 2015-2020 [*online]. [cit. 2018-07-01]. Dostupné z: https://www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf s. 5
27. *Parkerian Hexad*. [Online]. [cit. 2016 8 20]. Dostupné z: https://vputhuseeri.wordpress.com/2009/08/16/149/.
28. *POŽÁR, Josef. Informační bezpečnost*. Plzeň: AleščČeněk, 2005, s. 37.
29. POŽÁR, Jozef. *Vybrané hrozby informační bezpečnosti organizací.* [Online]. [cit. 6. července 2018]. Dostupné z: https://www.cybersecurity.cz/data/pozar2.pdf.
30. PROSISE, Chris a Kevin MANDIVA. *Incident response & computer forensics, 2. vyd.* Emeryville: McGraw-Hill, 2003, s. 13.
31. Před čím se chránit? - Bezpečnostní hrozby, události, incidenty. *[Online]. [cit. 2018-07-06]. Dostupné z: https://www.kybez.cz/bezpecnost/pred-cim-chranit*
32. *Příchod hackerů: příběh Stuxnetu.* [Online]. [cit. 2018-07-01]. Dostupné z: https://www.root.cz/clanky/prichod-hackeru-pribeh-stuxnetu/.
33. RAK, Roman. Homo sapiens a bezpečnost. ICT Forum/PERSONALIS 2006 [předneseno 27. září 2006]. Praha (prezentace na konferenci).
34. SCHNEIER, Bruce. [Online]. [cit. 2018-07-18]. Dostupné z: https://www.azquotes.com/quote/570039.
35. SCHNEIER, Bruce. [Online]. [cit. 2018-07-18]. Dostupné z: https://www.azquotes.com/quote/570035.
36. SCHNEIER, Bruce. [Online]. [cit. 2018-07-18]. Dostupné z: https://www.azquotes.com/quote/570047.
37. SCHNEIER, Bruce. [Online]. [cit. 2018-07-18]. Dostupné z: https://www.azquotes.com/quote/570040.
38. *Pokyny NIS.* [online]. [citováno 1. července 2018]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016L1148&from=EN.
39. SVOBODA, Ivan. *Řešení kybernetické bezpečnosti.* Přednáška na Akademii CRIF. (23. 9. 2014)
40. ŠÁMAL, Pavel a kol. *Trestní zákoník II. Komentář k §§ 140-421.* Vyd. 2. Praha: C. H. Beck, 2012, s. 2308
41. ŠULC, Vladimír. *Kybernetická bezpečnost.* Plzeň: AleščČeněk, 2018. s. 20 a násl.

42. *Zpravodajské služby: kampaň s cílem ovlivnit americké prezidentské volby nařídil Putin.* [online]. [cit. 2017 Jun 29]. Dostupné z: http://www.ceskatelevize.cz/ct24/svet/2005207-tajne-sluzby-kampan-ktera-mela-ovlivnit-prezidentske-volby-v-usa-naridil-putin
43. *Kompletní nabídka služeb kybernetické bezpečnosti společnosti CGI.* [online]. [citováno 2018-07-10]. Dostupné z: https://mss.cgi.com/service-portfolio
44. *Definice a aplikace protokolu TLP (TrafficLightProtocol).* [online]. [citováno 2018 Jan 13]. Dostupné z: https://www.us-cert.gov/tlp.
45. VALÁŠEK, Jarmil, František KOVÁŘÍK a kol. *Krizové řízení v nevojenských krizových situacích*. Praha: Ministerstvo vnitra - Generální ředitelství Hasičského záchranného sboru České republiky, 2008 [online]. [citováno 1. července 2018]. Dostupné z: http://www.hzscr.cz/soubor/modul-c-krizove-rizeni-pri-nevojenskych-krizovych-situacich-pdf.aspx.
46. WAISOVÁ, Šárka. *Bezpečnost: vývoj a koncepční změny.* Plzeň: AleščEněk, s.r.o., 2005. ISBN 80-86898-21-0.
47. *WannaCry se vůbec neměl šířit. Stačilo použít službu Windows Update.* [online]. [citováno 2017 Jun 27]. Dostupné z: https://www.zive.cz/clanky/wannacry-se-nemel-vubec-rozsirit-stacilo-abychom-pouzivali-windows-update/sc-3-a-187740/default.aspx
48. WIENER, Norbert. *Kybernetika: aneb řízení a komunikace v živých organismech a strojích.* Praha: Státní nakladatelství technické literatury, 1960. 148 s.
49. *Základní pojmy.* [online]. [citováno 2018-07-10]. Dostupné z: https://www.kybez.cz/bezpecnost/pojmoslovi.
50. ZEMAN, Petr a kol. *Česká bezpečnostní terminologie: výklad základních pojmů* [online]. [cit. 2018-07-10]. Dostupné z: http://www.defenceandstrategy.eu/filemanager/files/file.php?file=16048 . s. 13

Modul 5

Základy digitální forenzní analýzy

1. Úvod

Pátý modul je z velké části "fyzický" modul založený na dílně, který by měl být realizován ve třídě. Studentům budou předloženy různé situace, kdy došlo k narušení nebo jiné kybernetické hrozbě, a oni jí budou muset přijít na kloub.

1.1 Shrnutí kurzu

Modul Základy digitální kriminalistiky poskytuje teoretické a praktické využití těchto znalostí při shromažďování, analýze a uchovávání důkazů, což vede k jejich použití jako důkazu u soudu. Obsah obsažený v programu tohoto modulu vám umožní upevnit tento cíl.

1.2 Cíle kurzu

Cílem tohoto modulu je poskytnout teoretické znalosti o koncepcích počítačové forenziky a aplikovat tyto znalosti při shromažďování, analýze a uchovávání důkazů, což vede k jejich použití jako důkazu u soudu. Obsah obsažený v programu tohoto modulu vám umožní upevnit tento cíl tohoto modulu.

1.3 Obsah kurzu

Vzhledem k praktické povaze kurzu bude probíhat převážně v hodinách fyziky pod vedením instruktora. V rámci workshopu budou mít studenti za úkol zajistit místo činu a získat co nejvíce průkazných stop o průběhu incidentu, utrpěných ztrátách a možných stopách.

1.4 Cíle učení

- základní definice
- zajištění věcných důkazů
- zabezpečení digitálních důkazů
- použití důkazů u soudu

1.5 Potřebné vybavení a materiály

Počítačová místnost s přístupem na internet
1 Pen Disk (paměťová karta) < 8 GB
1 Pen Disk (paměťová karta) > 8 GB

1.6 Sylabus

Výsledek učení	Student, který úspěšně absolvuje tento modul, bude znát/umět následující.
NOVINKY	
W1	Student zná modely digitální forenzní analýzy
W2	Žák zná vztah mezi stopami, důkazy a zločinem.
DOVEDNOSTI	
U1	Student vypracovává forenzní zprávy
U2	Student na místě činu identifikuje, shromažďuje, získává a zajišťuje digitální důkazy pomocí různých technik, přičemž chrání neporušenost důkazů.
U3	Student uplatňuje osvědčené postupy a praktiky při získávání a zpracování digitálních důkazů.
U4	Student je obeznámen s různými technikami počítačové forenziky pro sběr a analýzu různých typů digitálních důkazů s využitím specifických technik a nástrojů.
SOUTĚŽE	
K1	Bude schopen pracovat jako člen nebo vedoucí vyšetřovacího týmu.

Obsah modulu (program přednášek a dalších aktivit)	**Odkaz na výsledky učení**
PŘEDNÁŠKY 1. pojmy, definice a modely WORKSHOPY 1. Zajištění a shromažďování digitálních důkazů na místech činu 2. Postupy pro získání digitálních důkazů a. Sterilizační postupy b. Akviziční techniky 3. Shromažďování a analýza informací 4. identifikace a analýza informací uložených v provozních systémech 5. Použití analytických nástrojů OpenSource 6. Případové studie z oblasti digitální forenzní analýzy a. Případová studie: Hacking pomocí nástrojů Windows SO	W1, W2 U1-4 K1

Metody ověřování výsledků učení									
Výsledek učení	Formy kreditních tříd								
	Ústní zkouška	Písemná zkouška	Částečný písemný úkol	Závěrečný písemný úkol (esej atd.)	Test	Projekt/prezentace	Nahlásit	Činnosti ve třídě	Ostatní ...
NOVINKY									
W1					x			x	
					x			x	
DOVEDNOSTI									
U1						x		x	
U2						x		x	
U3						x		x	
U4						x		x	
SOUTĚŽE									
K1						x		x	

Zůstatek kreditů ECTS		
Forma pracovního zatížení studentů		Počet hodin
Počet hodin s přímou účastí akademického pracovníka		
1.1	Účast na přednáškách	4
1.2	Účast na seminářích	
1.3	Účast na seminářích	30
1.4	Účast na laboratorních činnostech	
1.5	Účast na projektech	
1.6	Účast na konzultacích (2-3krát za semestr)	
1.7	Účast na konzultacích k projektu	
1.8	Účast na zkouškách/testech	2
1.9	Ostatní ...	
1.10	**Počet hodin strávených za přímé asistence akademických pracovníků (součet 1.1 - 1.9)**	26
1.11	**Počet ECTS kreditů, které student získal v hodinách vyžadujících přímou účast akademického pedagoga)**	1
Individuální práce studentů		
2.1	Individuální studium (včetně e-learningových přednášek)	20
2.2	Individuální příprava na semináře	10
2.3	Individuální příprava na test	
2.4	Individuální příprava na laboratorní výuku	
2.5	Příprava zpráv	
2.6	Realizace samostatně prováděných úkolů (projekty, dokumentace)	
2.7	Příprava na závěrečnou zkoušku/testy semináře	5
2.8	Příprava na závěrečnou zkoušku/testování přednášek	5
2.9	Další	
2.10	**Počet hodin individuální práce (součet 2.1 - 2.9)**	40
2.11	**Počet kreditů ECTS získaných studentem v rámci jednotlivých vzdělávacích aktivit**	1,5
Celková pracovní zátěž (h)		**66**

ECTS kredity za modul	2,5

Kritéria pro hodnocení kompetencí studentů
Minimální požadavky na tři skupiny výsledků učení, kterých musí student dosáhnout, aby předmět absolvoval, jsou uvedeny níže v syntetické podobě. Aby Student modul absolvoval, musí být všechny výsledky učení popsané v sylabu pozitivně ověřeny osobou (osobami), která (které) modul vyučuje (vyučují).

W - VĚDOMOSTI
Hodnocení:
Uspokojivý - Student si pamatuje a reprodukuje znalosti, které má v rámci modulu zvládnout.
Dobrý - Žák dodatečně interpretuje jevy / problémy a je schopen vyřešit typický problém.
Velmi dobře -Student je schopen řešit i složité problémy v dané oblasti, je schopen syntetizovat, provést komplexní hodnocení, vytvořit práci, která je originální a inspirativní pro ostatní.

U - DOVEDNOSTI
Hodnocení:
uspokojivý - student zná podstatu činností a je schopen pod vedením akademického učitele provádět činnosti/řešit problémy související s obsahem modulu.
Dobrý - Student je schopen samostatně provádět činnosti / úkoly / řešit typické problémy související s obsahem modulu.
Velmi dobře - Student si plně osvojil schopnost / dovednost provádět činnosti / úkoly / problémy stanovené v obsahu modulu, a to i ve složitějších případech.

K - SOCIÁLNÍ KOMPETENCE
Hodnocení:
uspokojivě - student pasivně vstřebává obsah modulu, prokazuje schopnost soustředit se a naslouchat.
Dobrý - Žák se aktivně účastní výuky, vytváří hodnotové soudy podle kritérií přijatých v daném oboru, dokáže aktivně spolupracovat ve skupině.
Velmi dobře - Žák integruje postoje podle navrženého modelu, rozvíjí vlastní systém profesních a společenských hodnot, je schopen převzít odpovědnost za jednání skupiny, včetně vedení.

2. Základní materiály pro učitele

- Všechny definice a klíčové poznámky jsou součástí prezentací.

3. Aktivity

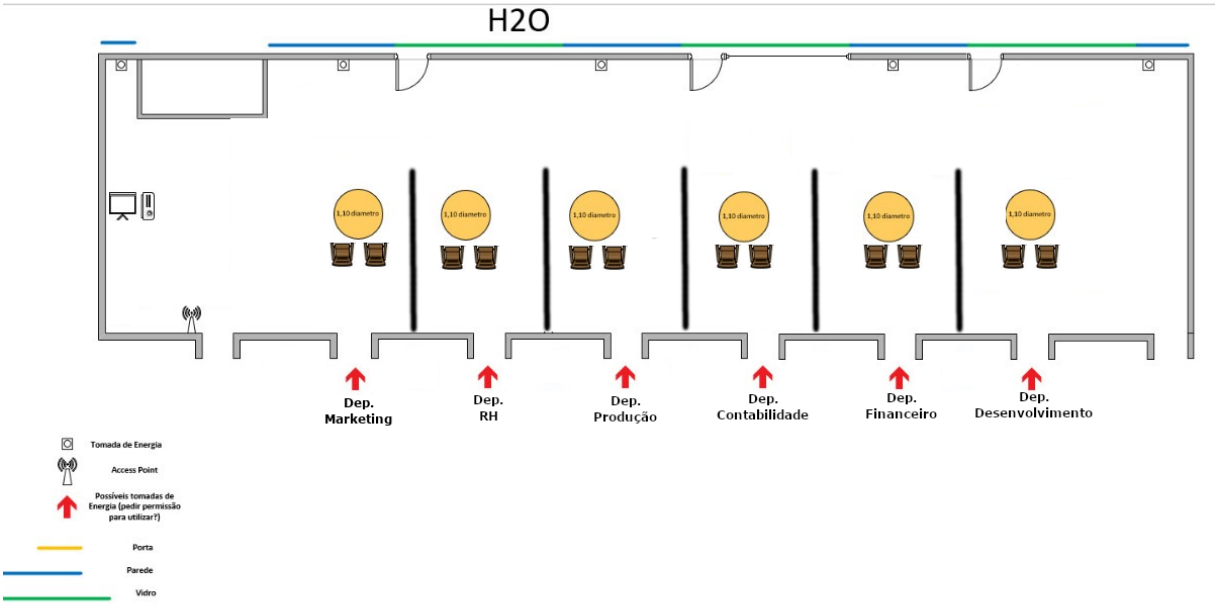
- **Diskuse** (kladení otázek) - tento typ otázek se používá k tomu, aby se studenti zamysleli nad postupy a významem digitální forenziky. Účastníci by měli k odpovědi dospět sami nebo prostřednictvím skupinových aktivit, jako je brainstorming.

  1- Když najdeme důležitý dokument v podezřelé složce na ploše, jak můžeme pochopit, jak byl dokument do této složky uložen? Jaké artefakty je třeba analyzovat?
  2- Když všechny indicie ukazují na použití cloudu k ukládání důležitých důkazů a známe přihlašovací údaje uživatele, musíme do tohoto cloudu vstoupit a analyzovat data, která jsou v něm obsažena?
  3- Postačí k analýze pevného disku systému Microsoft Windows použití sady Sleuth Kit? V jakém kontextu bychom měli použít jiné nástroje?

- **Vytváření a analýza artefaktů -** toto cvičení by mohlo být cvičením pro práci ve dvojicích/skupinách. Hlavním cílem je, aby tým vytvořil pouze jeden typ digitálního artefaktu a podělil se s druhým týmem o činnost, která s ním byla spojena. Druhý tým, který provádí analýzu, shromáždí forenzní důkazy z této činnosti. Když získají očekávané forenzní výsledky, vymění si role.

- **Vytváření stránek pro analýzu artefaktů** - Operační systémy neustále vytvářejí nové artefakty, které je třeba podrobit forenzní analýze. Tato analýza může být pro forenzní vyšetřovatele důležitou informací při jejich postupech.

- Cvičení na místě činu - Účelem tohoto cvičení je rozvíjet praktický obsah související s prací na místě činu/nehody a s prací u počítače s napájením (forenzní expertiza s živými daty). Je třeba připravit následující kroky:
    1. **Sestavení scénáře** - začíná pozváním / jmenováním studentů, kteří budou na místě přítomni s potřebnými nástroji, aby se stali součástí týmu pro sběr forenzních důkazů. Bude nutné připravit typ vyšetřovaného trestného činu, místo sběru, příslušné vybavení atd.
    2. **Příprava počítačů - Jedná se o** nejdůležitější fázi, kdy se připravují počítače s potřebnými artefakty, které budou studenti sbírat. Bude nutné vytvořit všechny artefakty a po přípravě prvního počítače duplikujeme nebo naklonujeme pevný disk pro potřebný počet počítačů podle scénáře.
    3. **Příprava prostoru** - Pokud jde o prostor pro postupy, je nutné mít co nejrealističtější scénář, jako například kterou část prostoru se síťovým směrovačem a internetem, s lidmi jako figuranty a podobně. Pomůže nakreslit prostor jako v příkladu níže:



Místností může být jen jedna místnost, ale v tomto případě se nabízela možnost, aby 6 týmů pracovalo najednou, což by jim zabralo méně času, ale zapojilo by se více lidí, kteří by působili jako vedoucí a pozorovali jednotlivé týmy.

4. Vyhodnocení - Každý tým před odpojením napájecího kabelu shromáždí všechny potřebné údaje a informace s jistotou úspěšné forenzní analýzy mrtvé schránky. Zařízení zůstane v péči každého týmu, dokud tým nedodá veškeré vybavení a zprávu o forenzní analýze. Hodnocení se zaměří na tuto zprávu.

4. **Internetové zdroje**

Elektronické vyšetřování na místě činu: Příručka pro první pomoc, druhé vydání (ojp.gov) - https://www.ojp.gov/pdffiles1/nij/219941.pdf

NIST SP 800-86 Příručka pro začlenění forenzních technik do **reakce na** incidenty https://doi.org/10.6028/NIST.SP.800-86.

Podvýbor pro digitální důkazy | NIST - https://www.nist.gov/organization-scientific-area-committees-forensic-science/digital-evidence-subcommittee

Vědecká pracovní skupina pro digitální, digitální a multimediální důkazy (digitální forenzní věda) jako forenzní vědní disciplína

DFIRScience - YouTube - https://www.youtube.com/c/DFIRScience

Soudní znalectví - start.me - https://start.me/p/q6mw4Q/forensics

Školení DFIR - https://dfir.training/

FSIDIIN | Forensic Science International: Digital Investigation | Journal | ScienceDirect.com by Elsevier - https://www.sciencedirect.com/journal/forensic-science-international-digital-investigation

5. **Zajímavé cyklické události**
   - **SANS CyberThreatIntelligenceSummit& Training [OnLine].**
   - **Mezinárodní konference IFIP WorkingGroup 11.9 o digitální kriminalistice [Arlington, USA].**
   - **General Police EquipmentExhibition& Conference (GPEC Digital) [Frankfurt, Německo].**
   - **Techno Security & Digital Forensics [Pasadena, USA].**
   - **Forensics Asia Expo [Jakarta, Indonésie].**
   - **Forensics Europe Expo [Londýn, Velká Británie].**
   - **Magnet Virtual Summit [OnLine].**
   - **Magnet User Summit [Nashville].**
   - **Národní konference o kyberkriminalitě [OnLine].**
   - **Mezinárodní konference o digitální kriminalistice a justici [OnLine].**
   - **Mezinárodní asociace forenzních věd (IAFS) [Sydney, Austrálie].**
   - **CongresoInformatica y Ciberseguridad 2023 [Madrid, Španělsko].**
   - **CHICYBERCON [Chicago, USA].**
   - **DFRWS - Digital ForensicResearch Workshop [Bonn, Německo].**
   - **Mezinárodní asociace počítačových specialistů (IACIS) [Orlando, Florida].**
   - **Konference ADFSL o digitální kriminalistice, bezpečnosti a právu**

6. Další otázky/testy

https://quizlet.com/ca/750977127/computer-and-digital-forensics-flash-cards/

7. Bibliografie

[1] BUNTING, Steve, The OfficialEnCE: EnCaseCertifiedExaminerStudy Guide, 2012.
[2] GRUNDY, Barry J., The Law Enforcement and ForensicExaminer'sIntroduction to Linux (http://www.linuxleo.com/Docs/linuxintro-LEFE-4.31.pdf), 2017.
[3] CASEY, Eoghan, Digital Evidence and ComputerCrime, Academicpress, 2011.
[4] BROWN, Christopher L. T., Computer evidence: Collection and Preservation, 2. vydání, 2009.
[5] CARVEY, Harlan, Investigating Windows Systems, 1. vydání, 2018.
[6] HALE LIGH, Michael, The Art of Memory Forensics: DetectingMalware and Threats in Windows, Linux, and Mac Memory 1. vydání, 2014.
[7] ENISA, Identification and handling of electronic evidence Toolset, září 2013.
[8] ENISA, Identification and handling of electronic evidence Handbook, září 2013.
[9] NIST, Computer Security Incident Handling Guide, Special Publication 800-61r2.

Modul 6

Komplexní zabezpečení sítě

1. Úvod

Modul Komplexní zabezpečení sítě se zaměřuje na hardwarové a softwarové metody prevence a detekce průniků a útoků. Představené metody by měly být široce využívány ve všech institucích a jejich znalost je nezbytná pro každého, kdo se chce zabývat kybernetickou bezpečností.

1.1 Cíle kurzu

Cílem tohoto modulu je seznámit studenty se základními způsoby ochrany místní sítě v jakékoli instituci. Tyto metody jsou široce dostupné, nevyžadují příliš specializované znalosti, a přesto umožňují výrazně zvýšit bezpečnost jakékoli sítě.

1.2 Obsah kurzu

Přednášková část kurzu bude probíhat převážně online, ačkoli vyučující může témata rozšířit v průběhu výuky.

1. Firewally
1.1 Úvod do firewallů
1.2 Potřeba brány firewall
1.3 Typy a vlastnosti firewallů
1.4 Topologie a architektury brány firewall
1.5 Příklady firewallů

2. systémy detekce narušení
2.1 Úvod do systémů detekce narušení
2.2 Typy a vlastnosti systémů detekce narušení
2.3 Implementační architektury pro systémy detekce narušení
2.4 Společná řešení a příklady systémů detekce narušení

3. systémy prevence narušení
3.1 Úvod do systémů prevence narušení
3.2 Typy a vlastnosti systémů prevence narušení

3.3 Implementační architektury systémů prevence narušení
4 Antivirus
4.1 Úvod do malwaru
4.2 Jak dochází k infekci malwarem
4.3 Nejčastější typy malwaru
4.4 Jak zjistit, odstranit a zabránit infekci malwarem
4.5 Zvláštní případ antivirového programu
4.6 Jak antivirový program funguje
4.7 Výběr správného antivirového softwaru

1.3 Cíle učení

1. Porozumět úloze firewallu v technologiích kybernetické bezpečnosti, jeho typům a funkcím, topologiím a architekturám a běžným řešením;
2. Porozumět úloze systémů detekce narušení v technologiích kybernetické bezpečnosti, jejich typům a vlastnostem, architekturám implementace a běžně používaným řešením;
3. Porozumět úloze systémů prevence narušení v technologiích kybernetické bezpečnosti, jejich typům a vlastnostem, architekturám implementace a běžně používaným řešením;
4. Pochopení úlohy antimalwaru v technologiích kybernetické bezpečnosti, způsobu šíření malwaru, různých typů malwaru, způsobu detekce, odstranění a prevence proti malwarovým infekcím, fungování konkrétního případu antimalwaru - antiviru - a jeho běžných řešení.

1.4 Potřebné vybavení a materiály

Počítačová místnost s přístupem na internet
Antivirový software

1.5 Sylabus

Výsledek učení	Student, který úspěšně absolvuje tento modul, bude znát/umět následující.
NOVINKY	
W1	Student zná princip fungování systémů firewall, IPS, IDS a antivirových programů.
W2	Student chápe význam používání vhodných ochranných opatření ve své instituci.
DOVEDNOSTI	
U1	Studenti budou schopni použít běžně dostupné metody pro detekci a prevenci průniků a útoků.
U2	Student je schopen najít slabá místa v kybernetické bezpečnosti instituce.
SOUTĚŽE	
K1	Student je schopen předat znalosti a kompetence týkající se základní bezpečnosti zaměstnancům své instituce.

Obsah modulu (program přednášek a dalších aktivit)	**Odkaz na výsledky učení**
PŘEDNÁŠKY 1. Firewally 2. systémy detekce narušení 3. systémy prevence narušení 4 Antivirové programy WORKSHOPY 1. konfigurace brány firewall 2. konfigurace systémů IDS a IPS 3. seznámení s antivirovým softwarem a jeho instalace 4. sledování statistik útoků a vyvozování závěrů	W1, W2 U1, U2 K1

Metody ověřování výsledků učení									
Výsledek učení	**Formy kreditních tříd**								
	Ústní zkouška	Písemná zkouška	Částečný písemný úkol	Závěrečný písemný úkol (esej atd.)	Test	Design/prezentace	Nahlásit	Činnosti ve třídě	Ostatní ...
NOVINKY									
W1					x			x	
W2					x			x	
DOVEDNOSTI									
U1						x		x	
U2						x		x	
SOUTĚŽE									
K1						x		x	

Zůstatek kreditů ECTS		
Forma pracovní zátěže studentů		Počet hodin
Počet hodin s přímou účastí akademického pracovníka		
1.1	Účast na přednáškách	4
1.2	Účast na seminářích	
1.3	Účast na seminářích	12
1.4	Účast na laboratorních činnostech	
1.5	Účast na projektech	
1.6	Účast na konzultacích (2-3krát za semestr)	
1.7	Účast na konzultacích k projektu	
1.8	Účast na zkouškách/testech	2
1.9	Ostatní ...	
1.10	**Počet hodin strávených za přímé asistence akademických pracovníků (součet 1.1 - 1.9)**	18
1.11	**Počet ECTS kreditů, které student získal v hodinách vyžadujících přímou účast akademického pedagoga)**	0,5
Individuální práce studentů		
2.1	Individuální studium (včetně e-learningových přednášek)	30
2.2	Individuální příprava na semináře	10
2.3	Individuální příprava na test	
2.4	Individuální příprava na laboratorní výuku	
2.5	Příprava zpráv	
2.6	Realizace samostatně prováděných úkolů (projekty, dokumentace)	
2.7	Příprava na závěrečnou zkoušku/testy semináře	10
2.8	Příprava na závěrečnou zkoušku/testování přednášek	5
2.9	Další	
2.10	**Počet hodin individuální práce (součet 2.1 - 2.9)**	55
2.11	**Počet ECTS kreditů, které student získal za jednotlivé výukové úkoly**	2
Celková pracovní zátěž (h)		**73**
ECTS kredity za modul		**2,5**

Kritéria pro hodnocení kompetencí studentů
Minimální požadavky na tři skupiny výsledků učení, kterých musí student dosáhnout, aby předmět absolvoval, jsou uvedeny níže v syntetické podobě. Aby Student modul absolvoval, musí být všechny výsledky učení popsané v sylabu pozitivně ověřeny osobou (osobami), která (které) modul vyučují.

W - VĚDOMOSTI
Hodnocení:
Uspokojivý - Student si pamatuje a reprodukuje znalosti, které má v rámci modulu zvládnout.
Dobrý - Žák dodatečně interpretuje jevy / problémy a je schopen vyřešit typický problém.
Velmi dobře -Student je schopen řešit i složité problémy v daném oboru, je schopen syntetizovat, provést komplexní hodnocení, vytvořit práci, která je originální a inspirativní pro ostatní.

U - DOVEDNOSTI
Hodnocení:
uspokojivý - student zná podstatu činností a je schopen pod vedením akademického učitele provádět činnosti/řešit problémy související s obsahem modulu.
Dobrý - Student je schopen samostatně provádět činnosti / úkoly / řešit typické problémy související s obsahem modulu.
Velmi dobře - Student si plně osvojil schopnost / dovednost provádět činnosti / úkoly / problémy

stanovené v obsahu modulu, a to i ve složitějších případech.

K - SOCIÁLNÍ KOMPETENCE
Hodnocení:
uspokojivě - student pasivně vstřebává obsah modulu, prokazuje schopnost soustředit se a naslouchat.
Dobrý - Žák se aktivně účastní výuky, vytváří hodnotové soudy podle kritérií přijatých v daném oboru, dokáže aktivně spolupracovat ve skupině.
Velmi dobře - Žák integruje postoje podle navrženého modelu, rozvíjí vlastní systém profesních a společenských hodnot, je schopen převzít odpovědnost za jednání skupiny, včetně vedení.

2. Základní materiály pro učitele

- Všechny definice a klíčové poznámky jsou součástí prezentací.

3. Aktivity

- Workshop o "hackování" webových stránek s ukázkou fungování bezpečnostních systémů

- Prezentace živých útoků a statistiky o tom, kolik z těchto útoků mohlo být zablokováno běžně dostupnými bezpečnostními metodami.

4. Internetové zdroje

- https://www.parallels.com/blogs/ras/types-of-firewalls/
- https://phoenixnap.com/blog/types-of-firewalls
- https://www.idc-online.com/technical_references/pdfs/data_communications/Firewall_Architectures.pdf
- https://phoenixnap.com/blog/intrusion-detection-system
- https://wisdomplexus.com/blogs/different-types-of-intrusion-detection-systems-ids/
- https://www.educba.com/types-of-intrusion-prevention-system/
- https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips
- https://www.snort.org/
- https://www.techtarget.com/searchsecurity/definition/malware
- https://www.crowdstrike.com/cybersecurity-101/malware/types-of-malware/

5. Zajímavé cyklické události

- Evropská konference o kybernetické bezpečnosti (https://eucybersecurity.com/)
- Oficiální summit o kybernetické bezpečnosti (https://cybersecuritysummit.com/)
- Každoroční zkušenost s kontrolním bodem CPX
- Cisco Live ALL IN (https://www.ciscolive.com/emea.html?zid=pp)
- Mezinárodní konference o bezpečnosti komunikací a sítí (http://www.iccns.org/)

6. Další otázky/testy

- https://quizlet.com/199055325/firewall-flash-cards/
- https://www.proprofs.com/quiz-school/topic/firewall
- https://quizlet.com/180954294/chapter-8-using-intrusion-detection-systems-flash-cards/

- https://quizlet.com/534059481/chapter-7-intrusion-detection-and-prevention-systems-flash-cards/
- https://quizlet.com/222087233/what-is-malware-flash-cards/
- https://quizlet.com/27987027/malware-flash-cards/
- https://www.gns3.com/
- https://www.brianlinkletter.com/open-source-network-simulators/

7. Bibliografie

1. Carter, E., & Hogue, J. (2006). *Základy prevence narušení*. Cisco Systems.
2. Chapman, D. B., & Zwicky, E. D. (1995). *Budování internetových firewallů*. Oreilly & Associates.
3. Grubb, S. (2021). *Jak kybernetická bezpečnost skutečně funguje: Praktický průvodce pro úplné začátečníky*. National Geographic Books.
4. Gupta, B., & Srinivasagopalan, S. (2020). *Handbook of research on intrusion detection systems (Příručka výzkumu systémů detekce narušení)*.
5. Guyer, J. P. (2017). *Úvod do systémů detekce narušení*. Createspace Independent Publishing Platform.
6. Komar, B., Beekelaar, R., & Wettern, J. (2003). *Firewally pro začátečníky*. For Dummies.
7. Mendoza, H. (2018). *Odstranění malwaru, spywaru a virů z počítače: Průvodce zvýšením bezpečnosti a rychlosti počítače odstraněním škodlivých virů, malwaru a spywaru*. Createspace Independent Publishing Platform.
8. Noonan, W., Noonan, W. J., & Dubrawsky, I. (2006). *Základy firewallu*. Cisco Press.
9. Pathan, A. K. (2016). Současný *stav v oblasti prevence a detekce narušení*. Auerbach Publications.
10. Verissimo, P. E. (2003). *Intrusion-Tolerant Architectures: Concepts and Design* [Magisterská diplomová práce]. https://www.di.fc.ul.pt/~nuno/PAPERS/TR-03-5.pdf